Symantec NetBackup™ SAN Client and Fibre Transport Guide

UNIX, Windows, Linux

Release 7.7

Symantec NetBackup™ SAN Client and Fibre Transport Guide

Documentation version: 7.7

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

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/

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, DVDs, 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_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing SAN Client and Fibre Transport

This chapter includes the following topics:

About NetBackup SAN Client and Fibre Transport

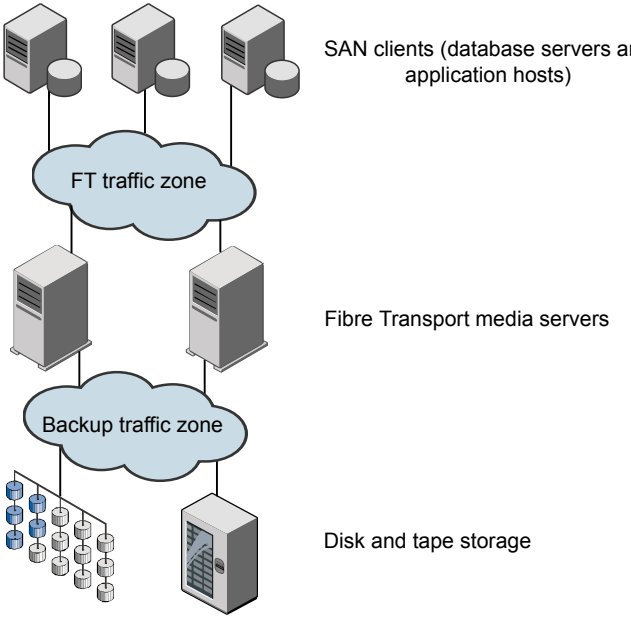
SAN Client is a NetBackup optional feature that provides high-speed backups and restores of NetBackup clients.

A SAN client is a special NetBackup client that can back up large amounts of data rapidly over a SAN connection rather than a LAN. For example, a database host can benefit from high-speed backups and restores. Fibre Transport is the name of the NetBackup high-speed data transport method that is part of the SAN Client feature.

The backup and restore traffic occurs over Fibre Channel, and the NetBackup server and client administration traffic occurs over the LAN.

Figure 1-1 shows a SAN Client configuration.

Figure 1-1 A SAN Client configuration



About Fibre Transport

NetBackup Fibre Transport is a method of data transfer. It uses Fibre Channel and a subset of the SCSI command protocol for data movement over a SAN rather than TCP/IP over a LAN. It provides a high-performance transport mechanism between NetBackup clients and NetBackup media servers.

Fibre Transport supports multiple, concurrent logical connections. The NetBackup systems that support Fibre Transport contain Fibre Channel HBAs that are dedicated to FT communication.

The NetBackup Fibre Transport service is active on both the SAN clients and the NetBackup media servers that connect to the storage.

Throughout this documentation, Fibre Transport connections between NetBackup clients and NetBackup servers are referred to as FT pipes.

About Fibre Transport media servers

A NetBackup FT media server is a NetBackup media server on which the Fibre Transport services are activated. NetBackup FT media servers accept connections from SAN clients and send data to the disk storage.

The host bus adapters (HBAs) that accept connections from the SAN clients use a special NetBackup target mode driver to process FT traffic.

The media server FT service controls data flow, processes SCSI commands, and manages data buffers for the server side of the FT connection. It also manages the target mode driver for the host bus adaptors.

Requires the SAN Client license.

About SAN clients

A NetBackup SAN client is a NetBackup client on which the Fibre Transport service is activated. The SAN client is similar to the NetBackup SAN media server that is used for the Shared Storage Option; it backs up its own data. However, the SAN client is based on the smaller NetBackup client installation package, so it has fewer administration requirements and uses fewer system resources.

Usually, a SAN client contains critical data that requires high bandwidth for backups. It connects to a NetBackup media server over Fibre Channel.

The NetBackup SAN Client Fibre Transport Service manages the connectivity and the data transfers for the FT pipe on the SAN clients. The SAN client FT service also discovers FT target mode devices on the NetBackup media servers and notifies the FT Service Manager about them.

About the Fibre Transport Service Manager

The FT Service Manager (FSM) resides on the NetBackup server that hosts the NetBackup Enterprise Media Manager service. FSM interacts with the FT services that run on SAN clients and on FT media servers. FSM discovers, configures, and monitors FT resources and events. FSM runs in the same process as EMM.

About NetBackup Release Notes

For information about supported systems and peripherals, limitations, and operational notes, see the *NetBackup Release Notes*:

http://www.symantec.com/docs/DOC5332

Chapter 2

Planning your deployment

This chapter includes the following topics:

Planning your SAN Client deployment

Table 2-1 provides an overview of planning your deployment of SAN Client and Fibre Transport.

Table 2-1 SAN Client deployment overview

Step	Deployment task	Section
Step 1	Read about best practices and operational notes	See "About SAN Client best practices" on page 14. See "SAN Client operational notes" on page 14.

Table 2-1 SAN Client deployment overview *(continued)*

Step	Deployment task	Section
Step 2	Determine the storage destination	See "About SAN Client storage destinations" on page 15.
Step 3	Determine the hosts to use	See "How to choose SAN Client and Fibre Transport hosts" on page 16.
Step 4	Prepare the SAN	See "Preparing the SAN" on page 21.
Step 5	License SAN Client	See "About the SAN Client license key" on page 26.
Step 6	Read about NetBackup agents	See "About NetBackup SAN Client support for agents" on page 16.
Step 7	Read about SAN Client and Hyper-V	See "About NetBackup SAN Client support for Windows Hyper-V Server" on page 17.
Step 8	Configure SAN Client and Fibre Transport	See "Configuring SAN Client and Fibre Transport" on page 28.
Step 9	Convert a SAN media server to a SAN Client	See "Converting a SAN media server to a SAN client" on page 19.

About SAN Client best practices

A Symantec tech note contains information about best practices for deployment. Symantec updates this tech note when new information becomes available. Symantec recommends that you read and following the practices that are described in the tech note, which is available at the following URL:

http://www.symantec.com/docs/TECH54778

SAN Client operational notes

The following items describe some operational items about which you should be aware:

- The NetBackup Client Encryption Option is not supported on UNIX and Linux SAN clients.
- Data compression or encryption can degrade Fibre Transport performance for backups and restores.

If you use data compression or encryption for backups, Fibre Transport pipe performance may degrade significantly for both backups and restores. In some configurations, compression may reduce performance by up to 95% of uncompressed performance.

About SAN Client storage destinations

You can use either disk or tape as a storage destination for the SAN Client and Fibre Transport feature.

NetBackup allows the storage devices to be connected to the FT media servers by any means.

About SAN Client disk storage destinations

For disk storage, a NetBackup OpenStorage implementation provides the greatest opportunity for high performance backups and restores. Those solutions can provide enough bandwidth and read and write speed to accept the large volume of data that the NetBackup Fibre Transport mechanism provides.

NetBackup media server deduplication is an OpenStorage implementation. NetBackup client-side deduplication is not supported.

About SAN Client tape storage destinations

SAN Client can use tape as a destination storage unit. Some tape drives are fast enough to read and write the large volume of data that the NetBackup Fibre Transport mechanism provides.

With tape as a destination you can use multistreaming, which divides automatic backups for a client into multiple jobs. Because the jobs are in separate data streams, they can occur concurrently. The data streams can be sent over one or more FT pipes to the FT media server. The media server multiplexes them together onto one or more tape media volumes. For example, if you have a database server that provides multiple streams of data, you can multistream those database backups to an FT media server. The FT media server multiplexes the data streams onto the media, increasing overall performance.

You can replace NetBackup SAN Media servers with SAN clients and continue to back up to tape. A SAN Client uses fewer system resources, both disk space and processor, than a SAN Media server.

To configure multistreaming, see the *NetBackup Administrator's Guide, Volume I*:

http://www.symantec.com/docs/DOC5332

SAN Client tape storage limitations

The following limitations exist for tape as a SAN Client storage destination:

- Only FT backups from the same client are multiplexed in a particular MPX group.
- FT backups from different clients are not multiplexed together in the same MPX group.
- You cannot multiplex different SAN clients to the same tape. Different clients can still be backed up to the same FT media server, but they are written to different tape drives in different MPX groups.
- FT and LAN backups (from the same client or different clients) are not multiplexed together in the same MPX group.
- SAN Client does not support Inline Tape Copy over Fibre Transport; Inline Tape Copy jobs occur over the LAN. The SAN Client features is designed for very high speed backup and restore operations. Therefore, SAN Client excludes backup options (such as Inline Tape Copy) that require more resources to process and manage.

How to choose SAN Client and Fibre Transport hosts

When you choose the systems to use for NetBackup Fibre Transport, be aware of the following:

- NetBackup SAN clients cannot also be NetBackup servers. Therefore, only configure a NetBackup client to be a SAN client on systems on which only the NetBackup client software is installed.
- Do not use the NetBackup master server as an FT media server. Data transfer consumes system resources and severely degrades NetBackup management performance.

About NetBackup SAN Client support for agents

The SAN Client feature uses shared memory for data transfer. If you use a NetBackup agent on a SAN client, the agent must have privileges to read and write from that shared memory.

Ensure that the agent has the appropriate privileges, as follows:

- On UNIX systems, install the NetBackup agent using the same user account under which NetBackup is installed.
- On Windows SAN clients, ensure that the NetBackup agent and the SAN Client Fibre Transport Service use the same account (that is, **Log On As**). The account

must have **Act as a part of the operating system** privilege enabled. By default, only the **Local System** account has the **Act as a part of the operating system** privilege enabled.

SAN Client does not support the following type of agent backups:

- Microsoft SharePoint
- Enterprise Vault
- Microsoft Exchange Database Availability Group (DAG) or Cluster Continuous Replication (CCR) backups through a passive node of an Exchange cluster.

About NetBackup SAN Client support for clustering

NetBackup supports SAN Clients in an application cluster. The following are the requirements for the SAN Clients that are in an application cluster:

- SAN Client must be installed on all failover nodes in the cluster.
- The FT client service and the Symantec PBX service must run on all failover nodes.
- The host computer operating system for each SAN client on each node must detect the FT media server target mode drivers.
- The NetBackup `LOCAL_CACHE` value must be `NO` on each SAN Client. By default, the value is not specified, so you must configure the value.

Warning: Do not change the `LOCAL_CACHE` value on the FT media servers or the master server.

See "Configuring SAN clients in a cluster" on page 45.

In the backup policy, you can use aliases or dynamic application cluster names for the references to the SAN client computers. NetBackup updates SAN client application cluster information every 5 minutes.

About NetBackup SAN Client support for Windows Hyper-V Server

NetBackup SAN Client supports backups over Fibre Transport for the Windows Hyper-V Server. Install the NetBackup client software on the Windows Hyper-V Server and then configure the SAN Client on the Hyper-V Server. Do not install the

NetBackup client software or configure the SAN Client on the operating systems within the Hyper-V virtual machines.

See "Configuring SAN clients" on page 41.

For backups, follow the procedures in the *NetBackup™ for Hyper-V Administrator's Guide* to create a Hyper-V policy to back up the Hyper-V Server and its virtual machines:

http://www.symantec.com/docs/DOC5332

If SAN client and Fibre Transport are configured correctly, backups occur over Fibre Transport.

NetBackup does not support Fibre Transport restores to the Windows Hyper-V Server. Restores occur over the LAN.

See "About NetBackup SAN Client unsupported restores" on page 18.

About NetBackup SAN Client unsupported restores

In most cases, if a backup uses the NetBackup Fibre Transport data transfer method, a restore also occurs by the Fibre Transport method.

However, NetBackup may not support Fibre Transport restores for some NetBackup options or for other products.

NetBackup does not support Fibre Transport restores for the following options:

Alternate client restores	SAN Client does not support alternate client restores to a LAN-based client. SAN Client does not support alternate client restores to a SAN-based client.
FlashBackup restores	SAN Client supports FlashBackup backups but restores occur over the LAN.
Windows Hyper-V restores	SAN Client supports backups over Fibre Transport but restores occur over the LAN. Depending on the options that you select when you configure the backup policy, you can restore the virtual machines and also individual files within the virtual machines. See "About NetBackup SAN Client support for Windows Hyper-V Server" on page 17.

About Fibre Transport throughput

The slowest speed of the following components may limit the Fibre Transport throughput rate:

- The speed capability of the SAN client.
  The speed with which the client reads and writes to the file system or database affects performance).
- The read and write speed of the storage unit.
- The bandwidth of the computer PCI I/O memory.
  On the SAN clients, a non-PCI-X card on the PCI-X bus of the HBA reduces the speed of the controlling bus. NetBackup FT performance may not be affected as much as on a media server, but performance may degrade to unacceptable levels.
- The speed of the Fibre Channel pipe that transports the data.
- The topology of the Fibre Channel.
  Bottlenecks may occur when multiple data streams are sent through a shared element such as a trunk or an inter-switch link.

Converting a SAN media server to a SAN client

Table 2-2 provides an overview of how to convert a SAN media server to a SAN client. The computer host name remains the same. This procedure assumes that all NetBackup server run a release that supports the SAN Client feature.

Table 2-2 How to convert from a SAN media server to a SAN client

Step	Task	Instructions
Step 1	Delete the SAN media server	Do the following: ■ In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Devices > Media Servers**. ■ Select the host. ■ Select **Actions > Enterprise Media Manager Database > Remove Device Host**.
Step 2	Uninstall the SAN media server software	See the *NetBackup Installation Guide for UNIX and Windows*: http://www.symantec.com/docs/DOC5332

Table 2-2 How to convert from a SAN media server to a SAN client *(continued)*

Step	Task	Instructions
Step 3	Prepare for Fibre Transport	Prepare the SAN for Fibre Transport and install the HBAs on the Fibre Transport hosts and SAN client hosts. See "Preparing the SAN" on page 21.
Step 4	Connect the storage to the FT media server host	Connect the SAN media server storage device to the FT media server for the new SAN client. For disk storage, mount the storage if necessary. See "Preparing the SAN" on page 21.
Step 5	Install the NetBackup media server software	Install the media server software on the hosts to function as Fibre Transport media servers. See the *NetBackup Installation Guide for UNIX and Windows*: http://www.symantec.com/docs/DOC5332
Step 6	Configure the FT media servers	See "Configuring SAN Client and Fibre Transport" on page 28.
Step 7	Install the NetBackup client software	Install the client software on the host that was the SAN media server. See the *NetBackup Installation Guide for UNIX and Windows*: http://www.symantec.com/docs/DOC5332
Step 8	Configure the SAN client	See "Configuring SAN Client and Fibre Transport" on page 28.
Step 9	Configure alternate server restore	Because the current host is no longer a media server, configure an alternate server restore and specify the FT media server as the **Restore server**. NetBackup then uses the FT media server to restore the images that were associated with the SAN media server. See **Media host override** in the **General Server** properties of the **Master Server Host Properties**. After all of the images that were associated with the SAN media server expire, you can unconfigure the alternate server restore.

Chapter 3

Preparing the SAN

This chapter includes the following topics:

Preparing the SAN

Table 3-1 shows the preparation steps and the order to perform them.

Table 3-1 SAN preparation overview

Step	Procedure	Section
Step 1	Zone the SAN	See "About zoning the SAN for Fibre Transport" on page 22.
Step 2	Install HBAs	See "About HBAs for SAN clients and Fibre Transport media servers" on page 24.
Step 3	Select HBA ports	See "When selecting the HBA ports for SAN Client" on page 24.
Step 4	Connect the fiber	See "About supported SAN configurations for SAN Client" on page 25.

About zoning the SAN for Fibre Transport

Before you can configure and use the NetBackup Fibre Transport (FT) mechanism, the SAN must be configured and operational.

See "About supported SAN configurations for SAN Client" on page 25.

For SAN switched configurations, proper zoning prevents Fibre Transport traffic from using the bandwidth that may be required for other SAN activity. Proper zoning also limits the devices that the host bus adapter (HBA) ports discover; the ports should detect the other ports in their zone only. Without zoning, each HBA port detects all HBA ports from all hosts on the SAN. The potentially large number of devices may exceed the number that the operating system supports.

Instructions for how to configure and manage a SAN are beyond the scope of the NetBackup documentation. However, the following recommendations may help you optimize your SAN traffic.

Table 3-2 describes the best practices for zoning the SAN on NetBackup appliances.

Table 3-2 Best practices for zoning the SAN on NetBackup appliances

Guideline	Description
One initiator per zone, multiple targets acceptable.	Symantec recommends that you create zones with only a single initiator per zone. Multiple targets in a single zone are acceptable, only if all of the targets are similar. Tape target resources should be in separate zones from disk target resources, regardless of initiator. However, both sets of resources may share the same initiator.
Be aware of performance degradation when a port is configured for multiple zones.	If you use a single port as an initiator or a target for multiple zones, this port can become a bottleneck for the overall performance of the system. You must analyze the aggregate required throughput of any part of the system and optimize the traffic flow as necessary.
For fault tolerance, spread connectivity across HBA cards and not ports.	To ensure the availability of system connections, if you incorporate a multi-path approach to common resources, pair ports on separate cards for like zoning. This configuration helps you avoid the loss of all paths to a resource in the event of a card failure.

Table 3-2 Best practices for zoning the SAN on NetBackup appliances *(continued)*

Guideline	Description
Zone the SAN based on WWN to facilitate zone migrations, if devices change ports.	It is recommended that you perform SAN zoning based on WWN. If switch port configurations or cabling architectures need to change, the zoning does not have to be recreated.

Table 3-3 describes the zones you should use for your SAN traffic.

Note: You must use physical port ID or World Wide Port Name (WWPN) when you specify the HBA ports on NetBackup Fibre Transport media servers.

See "How to identify the HBA ports" on page 31.

Table 3-3 Fibre Channel zones

Zone	Description
A Fibre Transport zone	A Fibre Transport zone (or backup zone) should include only specific HBA ports of the hosts that use Fibre Transport, as follows: ■ Ports on the FT media server HBAs that connect to the SAN clients. These ports use the Symantec target mode driver. See "About the target mode driver" on page 30. ■ Ports on the SAN client HBAs that connect to the media server ports that are in target mode. The ports on the SAN clients use the standard initiator mode driver. You must define the FT media server target ports by physical port ID or World Wide Port Name (WWPN). The target mode driver WWPNs are not unique because they are derived from the Fibre Channel HBA WWPN. The NetBackup SAN clients should detect only the HBA ports that are in target mode on the NetBackup media servers. They should not detect HBA ports in initiator mode on the NetBackup media servers. They should not detect the FC HBAs on other hosts. To promote multistream throughput, each SAN client should detect all target mode devices of the media server HBA ports in the zone.
External storage zone	If the storage is on a SAN, create an external storage zone. The zone should include the HBA ports for the storage and the FT media server HBA ports that connect to the storage. All of the ports in the storage zone use the standard initiator mode HBA driver.

About HBAs for SAN clients and Fibre Transport media servers

The Fibre Channel host bus adapter (HBA) and driver requirements differ on the SAN clients and on the NetBackup FT media servers, as follows:

HBAs on SAN clients	The HBAs on the SAN clients can be any supported Fibre Channel HBA. The HBA ports must operate in the default initiator mode. For the HBAs on the SAN client systems, do the following: ■ Install the drivers for the HBA. ■ Install the utilities for the HBA. Although not required for NetBackup operation, the utilities may help to troubleshoot connectivity problems.
HBAs on NetBackup FT media servers	The NetBackup media servers that host Fibre Transport require the following: ■ For the connections to the SAN clients, use a QLogic HBA that NetBackup supports for Fibre Transport. For these HBAs, you must configure them to use the NetBackup target mode driver. See "About nbhba mode and the ql2300_stub driver" on page 30. ■ If you use SAN attached storage, you can use any supported Fibre Channel HBA to connect to the storage. For these HBAs, you should install the QLogic driver and utilities. The HBA ports that connect to the storage must remain in the default initiator mode. ■ The HBAs and their drivers must support 256K size buffers for data transfer.

For information about supported HBAs, see the Hardware Compatibility List at the following URL:

http://www.netbackup.com/compatibility

When selecting the HBA ports for SAN Client

You must have adequate HBA ports in the FT media servers to support the FT pipes from the SAN clients. If you also use SAN attached storage, the media servers must have enough HBA ports to connect to the shared storage.

You must determine which ports to use for FT connections between the NetBackup media servers and the SAN clients, as follows:

- Determine which Fibre Channel HBAs you want to use for FT connections on the systems on which the NetBackup media servers are installed.
- Determine which Fibre Channel ports you want to use for FT connections on each SAN client.

All ports on QLogic HBAs must be either in target mode or initiator mode. You cannot connect one port on an HBA to a SAN client and another port to the storage.

About supported SAN configurations for SAN Client

NetBackup supports the following SAN configurations for Fibre Transport:

Node port (N_Port) switched configuration	Connect the NetBackup media servers and SAN clients to a SAN switch as follows: ■ Connect the HBA port on the NetBackup FT media server to a Fibre Channel switch port. ■ Connect each SAN client HBA port to ports on the same Fibre Channel switch. ■ Define the zones on the switch so that the client(s) and server(s) are in the same zone. Be aware of the following: ■ You must define the NetBackup FT media server target ports by physical port ID or World Wide Port Name (WWPN). The target mode driver WWPNs are not unique because they are derived from the Fibre Channel HBA WWPN. ■ You can define SAN client ports by either port ID or WWPN. However, if you use one method only, zone definition and management is easier.
Fibre Channel arbitrated loop (FC-AL) configuration	Use Fibre Channel arbitrated loop (FC-AL) to connect a NetBackup FT media server HBA port directly to a NetBackup SAN client HBA port. **Note:** FC-AL hubs are not supported.

Chapter 4

Licensing SAN Client and Fibre Transport

This chapter includes the following topics:

About SAN Client installation

No special installation is required for the core NetBackup Fibre Transport components. However, you must activate the feature by entering the SAN Client license key.

See "About the SAN Client license key" on page 26.

About the SAN Client license key

Enter the SAN Client license key on the NetBackup master server.

If the NetBackup Enterprise Media Manager server runs on a host other than the master server, also enter the license key on that host.

If the license key expires or is unavailable (such as in a disaster recovery situation), backups and restores occur over the LAN.

When upgrading SAN Client and Fibre Transport

When you upgrade NetBackup, all components are upgraded including the SAN client and Fibre Transport components.

For NetBackup upgrade installation instructions, see the *NetBackup Installation Guide for UNIX and Windows*:

http://www.symantec.com/docs/DOC5332

Chapter 5

Configuring SAN Client and Fibre Transport

This chapter includes the following topics:

Configuring SAN Client and Fibre Transport

To configure SAN Client and Fibre Transport, you must complete multiple procedures on multiple computers.

Table 5-1 shows the configuration steps and the order to perform them.

Table 5-1 SAN Client and Fibre Transport configuration process

Step	Task	Section
Step 1	Configure the FT media servers	See "Configuring a Fibre Transport media server" on page 29.
Step 2	Configure the SAN clients	See "Configuring SAN clients" on page 41. See "Configuring SAN clients in a cluster" on page 45.
Step 3	Configure FT properties	See "About configuring Fibre Transport properties" on page 47.
Step 4	Configure SAN client usage preferences	See "SAN client usage preferences" on page 54.

Configuring a Fibre Transport media server

Table 5-2 describes the process for configuring an FT media server.

Table 5-2 Process to configure an FT media server

Step	Task	Section
Step 1	Read the conceptual information about configuring an FT media server	This information that may help you avoid serious problems. See "About Linux concurrent FT connections" on page 52. See "About HBAs for SAN clients and Fibre Transport media servers" on page 24. See "About the target mode driver" on page 30. See "About nbhba mode and the ql2300_stub driver" on page 30. See "About FC attached devices" on page 30. See "How to identify the HBA ports" on page 31. See "About HBA port detection on Solaris" on page 32. See "About Fibre Transport media servers and VLANs" on page 33.
Step 2	Start `nbhba` mode on the media server	See "Starting nbhba mode" on page 33.
Step 3	Mark the HBA ports	See "Marking the Fibre Transport media server HBA ports" on page 35.
Step 4	Configure the FT services	See "Configuring the media server Fibre Transport services" on page 38.

About the target mode driver

On NetBackup FT media servers, QLogic Fibre Channel host bus adapter (HBA) ports connect to the NetBackup SAN clients. Symantec provides a special *target mode driver* for the ports on those HBAs. Those ports must operate in target mode; the target mode driver replaces the default, initiator mode driver. Target mode applies only to QLogic HBAs; the target mode configuration process affects only QLogic HBA ports.

After the target mode driver binds to the HBA ports, those ports appear as two **ARCHIVE Python** tape devices during SCSI inquiry. However, they are not tape devices and do not appear as tape devices in NetBackup device discovery. Each port appears as two tape devices because operating systems allow only one data stream per port. Two pseudo tape devices for each port increases throughput.

See "About Linux concurrent FT connections" on page 52.

See "About HBAs for SAN clients and Fibre Transport media servers" on page 24.

About nbhba mode and the ql2300_stub driver

The first step of the process to configure the media server HBA drivers is to start `nbhba` mode. The `nbhba` mode binds the Symantec provided `ql2300_stub` driver to all QLogic ISP2312 and ISP24*xx* HBA ports on the host.

The `ql2300_stub` driver prevents the standard initiator mode driver from binding to the ports. If the QLogic driver binds to the HBA ports, the NetBackup `nbhba` command cannot mark the ports that you want to operate in target mode. The target mode driver also cannot bind to the HBA ports.

The `ql2300_stub` driver also lets NetBackup read and modify the device ID in NVRAM of the QLogic ports. After you start `nbhba` mode and mark the ports of the QLogic HBAs that connect to the SAN clients, those ports operate in target mode.

The computer exits `nbhba` mode when the FT server starts.

Note: For Linux operating systems, warning messages may be displayed in the console or the system log when the `ql2300_stub` driver is loaded into the kernel.

See "Kernel warning messages when Symantec modules load" on page 71.

About FC attached devices

In `nbhba` mode, all devices that are attached to QLogic ISP2312 and ISP24*xx* HBA ports are unavailable. If disk or tape devices are attached to QLogic HBAs, those

devices become unavailable. They remain unavailable until you exit `nbhba` mode on that computer.

Warning: Do not configure HBAs on a computer that has a start device that is attached to a QLogic ISP2312 or ISP24*xx* port. If you do, the computer may become unbootable. If any critical file systems are mounted on any devices that are attached to a QLogic HBA, the computer also may become unbootable. Before you begin HBA configuration, dismount any file systems that are attached to a QLogic HBA.

To determine if devices are attached to QLogic HBAs, you should examine your devices and your mounted file systems.

You can configure the QLogic HBAs on a different NetBackup media server that does not contain a QLogic HBA connected start device. Then, you can install them in the NetBackup FT media servers and configure the FT services. Afterward, you should remove the `nbhba` driver from the media server on which you configured the HBAs.

See "Disabling a Fibre Transport media server" on page 62.

The process also ends `nbhba` mode on that computer.

How to identify the HBA ports

If the computer on which you mark ports contains multiple HBAs, it may be difficult to determine how the World Wide Names (WWNs) relate to the HBAs. The NetBackup `nbhba` command that marks the HBA ports requires the port WWN. The port WWN also may be known as the World Wide Port Name (WWPN).

To avoid problems, you can install all of the QLogic HBAs in a NetBackup media server that has no other Fibre Channel HBAs installed. You can mark all HBA ports and then install the HBAs in the appropriate NetBackup media servers.

Warning: A QLogic HBA may exist as a chipset on a motherboard. To avoid problems, you should determine if the computer contains built-in QLogic ports.

If you cannot mark ports in a computer that has only the QLogic HBAs that you want to mark, the following may help:

- The HBA may identify the port WWNs on the card. Examine the HBA for the WWNs.
- The Fibre Channel switch may display WWNs for attached and operational HBA ports.

- The SAN utility software may provide the capability to list the WWNs of the HBA ports.
- On Solaris 10, you can list WWNs for native drivers by using the `fcinfo hba-port` command.
- The NetBackup `nbhba` command `-l` option lets you compare the port WWN addresses easily. (The computer must be in `nbhba` mode.) For the QLA-234x series, the port WWNs on the same card differ in the second byte and the sixth byte. The following example shows two, two-port HBAs. Lines 1 and 2 are one HBA; lines 3 and 4 are the other HBA.

```
/usr/openv/netbackup/bin/admincmd/nbhba -l
1 2312 21:00:00:E0:8B:83:9D:A1 "QLA2342 " 0 0 101
2 2312 21:01:00:E0:8B:A3:9D:A1 "QLA2342 " 1 0 101
3 2312 21:00:00:E0:8B:8F:28:7B "QLA2342 " 0 0 101
4 2312 21:01:00:E0:8B:AF:28:7B "QLA2342 " 1 0 101
```

  This output also shows that the ports are in initiator mode. The second rightmost column shows 0, and the rightmost column does not begin with 8.
- If the HBA contains LEDs on the metal mounting bracket, the color changes to green after you mark a port (yellow is initiator mode). (The computer must be in `nbhba` mode.) You can see if you marked the ports in the correct card. If you did not, you can return those ports to initiator mode and then mark other ports until you mark the correct ones.

About HBA port detection on Solaris

On systems earlier than Solaris 10 Update 7, NetBackup detects the PCI bus and allows ports on one bus only to be used for target mode.

The following is the port detection behavior on systems earlier than Solaris 10 Update 7:

- The first choice is the bus with the most 2312 target mode ports.
- If there are no 2312 target mode ports, the bus with the most 24xx target mode ports is used.
- Target mode ports on other busses are not used.

Beginning with Solaris 10 Update 7 and Solaris 11, target ports on more than one bus are supported.

About Fibre Transport media servers and VLANs

For an FT media server that has multiple network interfaces for VLANs, NetBackup must recognize the primary network interface of the host before any other network interfaces for the host. Each NetBackup host recognizes other NetBackup hosts by using its **Additional Servers** list. The **Additional Servers** list appears in the **NetBackup Administration Console** host properties **Servers** page for that host.

Ensure that the FT server's primary host name appears before any other interface names for that FT media server host. Do so in the **Additional Servers** lists of the following NetBackup hosts:

- The master server.
- The FT media server.
- All of the SAN clients that the FT media server backs up.

You may be able to use operating system commands to determine the primary interface. UNIX-type operating systems have a `hostname` command, which displays the short name of the primary interface. They also have a `domainname` command, which shows the domain name of the primary interface. On Windows, you can use the i`pconfig -all` command to display host and domain information.

See "Backups failover to LAN even though Fibre Transport devices available " on page 70.

Starting nbhba mode

Before you mark HBA ports, you must start `nbhba` mode, which binds the `ql2300_stub` driver to the QLogic HBA ports.

To start `nbhba` mode, see the following:

- To start `nbhba` mode on Linux
- To start `nbhba` mode on Solaris

You must be the root user.

To start `nbhba` mode on Linux

1. Ensure that the HBAs are not connected to the SAN.
2. Invoke the `nbftsrv_config -nbhba` command and option. The computer enters `nbhba` mode. The following is an example; output on your system may differ:

```
/usr/openv/netbackup/bin/admincmd/nbftsrv_config -nbhba
Installing nbhba driver.
Are you sure you want to unload QLogic driver: qla2300? [y,n]
(y)
```

3. Answer **y** to unload the QLogic driver. The process continues as follows:

```
Removing qla2300
```

Note: For Linux operating systems, warning messages may be displayed in the console or the system log when the `ql2300_stub` driver is loaded into the kernel.

See "Kernel warning messages when Symantec modules load" on page 71.

---

4. Continue by marking the HBA ports.

See "Marking the Fibre Transport media server HBA ports" on page 35.

To start `nbhba` mode on Solaris

1. Ensure that the HBAs are not connected to the SAN.
2. Invoke the `nbftsrv_config -nbhba` command and option. The computer enters `nbhba` mode. The following is an example; output on your system may differ:

```
/usr/openv/netbackup/bin/admincmd/nbftsrv_config -nbhba
Installing nbhba driver.
Waiting for driver references to ql2300_stub to free up (this
may take some time).
The following driver aliases need to be removed:
qlc "pci1077,2312.1077.10a"
Would you like to run update_drv to remove these now? [y,n] (y)
```

3 Answer **y** to remove any driver aliases. The process continues as follows:

```
/usr/sbin/update_drv -v -d -i "pci1077,2312.1077.10a" qlc
Done copying driver into system directories.
Done adding driver.
MUST REBOOT TO COMPLETE INSTALLATION.
```

4 Reboot the host.

5 Continue by marking the HBA ports.

See "Marking the Fibre Transport media server HBA ports" on page 35.

Marking the Fibre Transport media server HBA ports

You must mark the ports on the QLogic HBAs that you want to operate in target mode. The process modifies the port device IDs in NVRAM. When the FT server starts, the NetBackup target mode driver binds automatically to the QLogic HBA ports that you marked.

Before you mark ports, you must start `nbhba` mode.

See "Starting nbhba mode" on page 33.

The following procedures describe how to mark the HBA ports and if necessary how to reverse this process and return the ports to the initiator mode driver:

- To mark the HBA ports
- To revert to the initiator mode driver

You must be the root user to make these changes.

To mark the HBA ports

1. Display the QLogic HBA ports on the media server by using the `nbhba` command with the `-l` option. The following is an example; output on your system may differ:

   ```
   /usr/openv/netbackup/bin/admincmd/nbhba -l
   1 2312 21:00:00:E0:8B:83:9D:A1 "QLA2342 " 0 0 101
   2 2312 21:01:00:E0:8B:A3:9D:A1 "QLA2342 " 1 0 101
   3 2312 21:00:00:E0:8B:8F:28:7B "QLA2342 " 0 0 101
   4 2312 21:01:00:E0:8B:AF:28:7B "QLA2342 " 1 0 101
   ```

   For the QLA-234x series, the port WWNs on the same card differ in the second byte and the sixth byte. This output shows two, two-port HBAs. Lines 1 and 2 are one HBA; lines 3 and 4 are the other HBA. The HBAs are in initiator mode: the second rightmost column shows 0, and the rightmost column does not begin with 8.

   Alternatively, use the `nbhba -L` option to produce verbose output, which lets you identify the mode more easily.

2. Mark the ports by using the `nbhba` command. The following is the syntax:

   ```
   /usr/openv/netbackup/bin/admincmd/nbhba -modify -wwn string
   -mode target
   ```

   For example, the following two commands change the two ports on one of the HBAs from the example output in step 1:

   ```
   nbhba -modify -wwn 21:00:00:E0:8B:8F:28:7B -mode target
   nbhba -modify -wwn 21:01:00:E0:8B:AF:28:7B -mode target
   ```

3 Verify the changes by using the `nbhba` command and -L option to display the HBA card ports on the server. The following is an example; output on your system may differ:

```
/usr/openv/netbackup/bin/admincmd/nbhba -L
HBA Port #1
 Device ID = 2312
 World Wide Name = 21:00:00:E0:8B:83:9D:A1
 Model Name = "QLA2342 "
 Port = 0
 Mode = initiator (designated for other use)(101)
HBA Port #2
 Device ID = 2312
 World Wide Name = 21:01:00:E0:8B:A3:9D:A1 "QLA2342
 Model Name = "QLA2342 "
 Port = 1
 Mode = initiator (designated for other use)(101)
HBA Port #3
 World Wide Name = 21:00:00:E0:8B:8F:28:7B
 Slot = ""
 Port = 0
 Fibre Not Attached
 Mode = target (designated for FT Server)(8101)
HBA Port #4
 World Wide Name = 21:01:00:E0:8B:AF:28:7B
 Slot = ""
 Port = 1
 Fibre Not Attached
 Mode = target (designated for FT Server)(8101)
```

The `nbhba -l` option also produces the output that lets you identify the mode:

```
/usr/openv/netbackup/bin/admincmd/nbhba -l
1 2312 21:00:00:E0:8B:83:9D:A1 "QLA2342 " 0 0 101
2 2312 21:01:00:E0:8B:A3:9D:A1 "QLA2342 " 1 0 101
3 2312 21:00:00:E0:8B:8F:28:7B "QLA2342 " 0 1 8101
4 2312 21:01:00:E0:8B:AF:28:7B "QLA2342 " 1 1 8101
```

The rightmost two columns show the ports that are marked for target mode: the second rightmost column shows 1, and the rightmost column begins with 8. The other digits in the rightmost column are not significant.

4 If necessary, transfer the HBAs to the appropriate media servers.

5 If necessary, connect the HBAs to the SAN.

6 Continue by configuring the FT services.

See "Configuring the media server Fibre Transport services" on page 38.

To revert to the initiator mode driver

- Invoke the `nbhba` command on the NetBackup FT server in which the HBA is installed. The following is the command syntax:

```
/usr/openv/netbackup/bin/admincmd/nbhba -modify -wwn
world_wide_port_name -mode initiator
```

Configuring the media server Fibre Transport services

You must configure the media server FT services before you configure the SAN clients. The FT server must run on the media servers so that the client operating system discovers the target mode driver (the FT device). Two services (nbftsrvr and nbfdrv64) comprise the NetBackup FT server that runs on media servers.

The `nbftsrv_config` script configures the media server for Fibre Transport. In this process, the script does the following:

- Installs the required drivers
- Installs the FT server start-up scripts
- Starts the FT server
  When the FT server starts, the NetBackup target mode driver binds automatically to the QLogic HBA ports that you marked. (The default QLogic driver is bound already to the ports that are not marked.) The HBA ports operate in target mode until you configure them to use the standard initiator mode again.
- Ends the `nbhba` mode on the computer (if it was in `nbhba` mode)

Configure the FT services on every NetBackup media server that connects to SAN clients.

For procedures, see the following:

- To configure Fibre Transport services on Linux
- To configure Fibre Transport services on Solaris

You must be the root user.

To configure Fibre Transport services on Linux

1 Run the `nbftsrv_config` script. The following is an example; output on your system may differ:

```
/usr/openv/netbackup/bin/admincmd/nbftsrv_config
Installing the Jungo driver and Fibre Transport Server.
The following automatic startup and shutdown scripts
(respectively) have been installed.  They will cause the
NetBackup Fibre Transport Server daemon to be automatically shut
down and restarted each time the system boots.
/etc/rc.d/rc2.d/S21nbftserver
/etc/rc.d/rc3.d/S21nbftserver
/etc/rc.d/rc5.d/S21nbftserver
/etc/rc.d/rc0.d/K03nbftserver
/etc/rc.d/rc1.d/K03nbftserver
/etc/rc.d/rc6.d/K03nbftserver
It may be necessary to temporarily unload your QLogic drivers
to free up the ports for the nbhba drivers.
This is an optional step.  If you choose not to do this, you may
not have access to all of the HBA ports until a subsequent
reboot.
Would you like to uninstall and reinstall your native QLogic
drivers now? [y,n] (y) y
```

2 The Qlogic drivers must be unloaded temporarily so that the stub driver (ql2300_stub) can bind to the marked HBA ports during this session.

If you answer `y`, you do not have to reboot the computer during this configuration process. However, any critical devices that are attached to QLogic HBAs in the computer may be unavailable during this session. To ensure that the critical devices remain available, answer `n`. Then, you must reboot when prompted. The stub driver binds to the marked ports during the boot process, and the default QLogic drivers bind to the unmarked ports.

If you answer `n`, go to step 5.

If you answer `y`, you are prompted again to unload each QLogic driver, as follows:

```
Are you sure you want to unload QLogic driver: qla2300? [y,n]
(y) y
```

3 To unload the QLogic driver, answer `y`. The process continues as follows:

```
Removing qla2300
Adding qla2300.
Adding qla2xxx.
Would you like to start the SANsurfer agent (qlremote)? [y,n]
(y) y
```

4 If the QLogic SANsurfer agent was loaded, the configuration process asks if you want to start the agent. To start the QLogic SANsurfer agent, answer `y`. The process continues as follows:

```
Starting qlremote agent service
Started SANsurfer agent.
/etc/udev/permissions.d/50-udev.permissions updated with Jungo
WinDriver permissions.
NetBackup Fibre Transport Server started.
Would you like to make these changes persist after a reboot?
[y,n] (y) y
```

5 To ensure that the FT server always starts after a computer reboot, answer `y`. The process continues as follows:

```
Running mkinitrd.  Previous initrd image is saved at
/boot/initrd-2.6.9-11.ELsmp.img.05-21-07.11:24:03.
```

If you answered `y` in step 2, the FT services are started, and the target mode driver binds to the marked HBA ports.

6 If you answered `n` in step 2, reboot the computer when prompted.

The FT services are started, and the target mode driver binds to the marked HBA ports.

To configure Fibre Transport services on Solaris

1 Run the `nbftsrv_config` script. The following is an example; output on your system may differ:

```
/usr/openv/netbackup/bin/admincmd/nbftsrv_config
Installing the Jungo driver and Fibre Transport Server.
Waiting for driver references to ql2300_stub to free up (this
may take some time).
The following automatic startup and shutdown scripts
(respectively) have been installed.  They will cause the
NetBackup Fibre Transport Server daemon to be automatically shut
down and restarted each time the system boots.
/etc/rc2.d/S21nbftserver
/etc/rc0.d/K03nbftserver
Adding "pci1077,2312.1077.101" to qlc.
No third party drivers found with conflicting driver aliases.
Done copying driver into system directories.
Done adding driver.MUST REBOOT TO COMPLETE INSTALLATION.
```

2 Reboot the host.

The FT services are started, and the target mode driver binds to the marked HBA ports.

Configuring SAN clients

Table 5-3 shows the steps to configure SAN clients.

Table 5-3 SAN Client and Fibre Transport configuration process

Step	Task	Section
Step 1	Configure firewalls on SAN clients	See "About configuring firewalls on SAN clients" on page 41.
Step 2	Configure SAN client drivers	See "SAN client driver requirements" on page 42.
Step 3	Configure the SAN client FT service	See "Configuring the SAN client Fibre Transport service" on page 43.

About configuring firewalls on SAN clients

NetBackup SAN clients require connectivity to the NetBackup master server and the NetBackup Enterprise Media Manager server.

Therefore, you must ensure that any firewall (software or hardware) allows the clients to communicate with the NetBackup master server and the EMM server. Normally, the NetBackup master server hosts the EMM server, so you may only have to allow communication with one system.

SAN client driver requirements

The operating systems of the NetBackup SAN clients may require device drivers that allow SCSI pass-through methods for the Fibre Transport traffic.

If the SAN client operating system is configured correctly, it recognizes each media server HBA port in target mode as two ARCHIVE Python devices.

Table 5-4 lists the driver requirements for each supported SAN client operating system.

Table 5-4 SAN client operating system driver requirements

Operating system	Driver requirements
AIX	Client systems require the standard tape driver. The driver should work without modification. For information about how to configure the driver, see the *NetBackup Device Configuration Guide*, available at the following URL: http://www.symantec.com/docs/DOC5332
HP-UX	Client systems require the `sctl` driver and pass-through device files. For information about how to configure the driver, see the *NetBackup Device Configuration Guide*, available at the following URL: http://www.symantec.com/docs/DOC5332
Linux	Client systems require the SCSI Generic (`sg`) driver and pass-through device files. For information about how to configure the driver, see the *NetBackup Device Configuration Guide*, available at the following URL: http://www.symantec.com/docs/DOC5332

Table 5-4 SAN client operating system driver requirements *(continued)*

Operating system	Driver requirements
Solaris	You must modify the `/kernel/drv/st.conf` file so that Solaris recognizes the FT devices on the NetBackup media servers. For information about how to do so, see the *NetBackup Device Configuration Guide*, available at the following URL: http://www.symantec.com/docs/DOC5332
Windows	A device driver is not required. The media server FT devices appear in the Windows Device Manager "Other devices" section as ARCHIVE Python SCSI Sequential Devices.

Some operating systems require specific patch and driver updates. For information about them, see the *NetBackup Release Notes*:

http://www.symantec.com/docs/DOC5332

Configuring the SAN client Fibre Transport service

You must enable the SAN Client Fibre Transport Service on the NetBackup clients that you want to function as SAN clients. During this process, the SAN client operating system discovers the FT devices on the FT media servers.

Warning: NetBackup SAN clients cannot also be NetBackup servers. Therefore, only configure a client to be a SAN client on systems on which the NetBackup client software only is installed.

See "Configuring SAN clients in a cluster" on page 45.

See "Registering a SAN client cluster virtual name" on page 46.

To configure a NetBackup client to be a SAN client

1 Verify that the Symantec PBX service is active on the client, as follows:

- On UNIX and Linux systems, run theNetBackup `bpps -x` command and verify that the `pbx_exchange` process is active.

- On Windows systems, use the Computer Management console to verify that the Symantec Private Branch Exchange service is active.

2 On the client, run the following command to enable the SAN Client Fibre Transport Service (`nbftclnt`):

UNIX and Linux:

```
/usr/openv/netbackup/bin/bpclntcmd -sanclient 1
```

Windows:

```
install_path\NetBackup\bin\bpclntcmd.exe -sanclient 1
```

3 Do the following to start the SAN client FT service:

- Linux: Boot the system, which also begins operating system device discovery. (Alternatively, you can run the NetBackup `bp.start_all` command to start the client FT service.)
- AIX, HP-UX, and Solaris: Run the NetBackup `bp.start_all` command. The command resides in the following directory:
  /usr/openv/netbackup/bin
- Windows: Boot the system, which also begins operating system device discovery.

4 On the systems that were not booted in step 3, perform the action that forces the SAN client operating system to discover devices.

The operating system must discover two FT devices for each media server HBA port that is in target mode.

The SAN Client Fibre Transport Service (`nbftclnt`) validates the driver stack functionality during device discovery. If validation fails, Fibre Transport is not enabled on the client.

See "SAN client Fibre Transport service validation" on page 72.

After the client OS discovers the FT devices, the SAN client is registered with NetBackup. You should not have to add the SAN client either manually or by using the Device Configuration Wizard.

5 If the client system does not discover the FT devices, verify the following:

- The Fibre Channel driver is installed on the SAN client.
- The SAN client HBA port is active on the Fibre Channel switch.
- The media server HBA port is active on the Fibre Channel switch.
- The SAN client is logged into the Fibre Channel switch name server.
- The FT media server is logged into the Fibre Channel switch name server.

- The FT media server port is zoned with the SAN client port.
- The zone is included in the active configuration.

Alternatively, you can try a scan operation for FT devices on a client system.

See "Rescanning for Fibre Transport devices from a SAN client" on page 57.

Configuring SAN clients in a cluster

The SAN Client FT service is not a cluster application. To protect the SAN clients that are in a cluster, you must configure all of the SAN clients in the cluster correctly.

See "Setting NetBackup configuration options by using the command line" on page 46.

Table 5-5 Process to configure a SAN client in a cluster

Step	Action	Description
Step 1	Install the NetBackup client software on each failover node	See the *NetBackup Installation Guide for UNIX and Windows*: http://www.symantec.com/docs/DOC5332
Step 2	Configure the SAN client on each failover node	Ensure that the FT service is active on all of the failover nodes. See "About configuring firewalls on SAN clients" on page 41. See "SAN client driver requirements" on page 42. See "Configuring the SAN client Fibre Transport service" on page 43.
Step 3	Register the virtual node name with the EMM server	See "Registering a SAN client cluster virtual name" on page 46.
Step 4	Configure the NetBackup local cache	On each SAN Client in the cluster, set the NetBackup `LOCAL_CACHE` option to `NO`. See "About NetBackup SAN Client support for clustering" on page 17. See "Setting NetBackup configuration options by using the command line" on page 46. **Warning:** Do not change the `LOCAL_CACHE` value on the FT media servers or the master server.

Registering a SAN client cluster virtual name

If you use a cluster to protect a client, you must register the cluster virtual name with the NetBackup Enterprise Media Manager.

See "Configuring SAN clients in a cluster" on page 45.

To register a cluster virtual name

1. Add the virtual name to the EMM database. The following is the command syntax:

   `nbemmcmd -addhost -machinename virtual_name -machinetype app_cluster`

   The following is the path to the `nbemmcmd` command:

   - UNIX: /usr/openv/netbackup/bin/admincmd
   - Windows: *install_path*\Program Files\VERITAS\NetBackup\bin\admincmd

2. For every client in the node, update the host so the virtual name is linked to the client host name. The following is the command syntax:

   `nbemmcmd -updatehost -add_server_to_app_cluster -machinename client_name -clustername virtual_name`

Setting NetBackup configuration options by using the command line

Symantec recommends that you use the **NetBackup Administration Console Host Properties** to configure NetBackup properties.

However, some properties cannot be set by using the **Administration Console**. You can set those properties by using the `bpsetconfig` command on NetBackup servers or the `nbsetconfig` command on NetBackup clients. Configuration options are key and value pairs, as shown in the following examples:

- `CLIENT_READ_TIMEOUT = 300`
- `LOCAL_CACHE = NO`
- `RESUME_ORIG_DUP_ON_OPT_DUP_FAIL = TRUE`
- `SERVER = server1.NetBackup`

You can specify some options multiple times, such as the `SERVER` option.

Use the `bpgetconfig` command for NetBackup servers or the `nbgetconfig` command for NetBackup clients to view and set configuration options.

To set configuration options by using the command line

1 In a command window or shell window on the host on which you want to set the property, invoke one of the following commands:

UNIX NetBackup client	`/usr/openv/netbackup/bin/nbsetconfig`
Windows NetBackup client	*`install_path`*`\NetBackup\bin\nbsetconfig.exe`
UNIX NetBackup server	`/usr/openv/netbackup/bin/admincmd/bpsetconfig`
Windows NetBackup server	*`install_path`*`\NetBackup\bin\admincmd\bpsetconfig.exe`

2 At the command prompt, enter the key and the value pairs of the configuration options that you want to set, one pair per line.

You can change existing key and value pairs.

You can add key and value pairs.

Ensure that you understand the values that are allowed and the format of any new options that you add.

3 To save the configuration changes, type the following, depending on the operating system:

Windows: `Ctrl + Z Enter`

UNIX: `Ctrl + D Enter`

About configuring Fibre Transport properties

NetBackup Fibre Transport properties control how your SAN clients use the Fibre Transport services for backups. NetBackup uses a hierarchy of properties to provide increasingly granular control of how your clients use NetBackup Fibre Transport. The following table describes the levels of property configuration in the **Host Properties** of the **NetBackup Administration Console**.

Table 5-6 Fibre Transport properties

Granularity	Description
Global FT properties for all SAN clients	Global FT properties apply to all SAN clients. Global FT properties are configured on the master server. Configure these properties in **Host Properties** > **Master Servers** in the **NetBackup Administration Console**.
FT properties for a media server or media servers	FT properties for a media server or servers apply to the SAN clients that the media server or servers back up. The properties override the global FT properties that are configured on the master server. Configure these properties in **Host Properties** > **Media Servers** in the **NetBackup Administration Console**. the master server **Fibre Transport**
FT properties for a SAN client or SAN clients	FT properties for a client or clients apply to the specific SAN client or clientss. FT properties for SAN clients override the media server FT properties. Configure these properties in **Host Properties** > **Clients** in the **NetBackup Administration Console**.

See "Configuring Fibre Transport properties" on page 48.

NetBackup provides one finer level of granularity for Fibre Transport. SAN client usage preferences override the FT properties that you configure through **Host Properties**.

See "SAN client usage preferences" on page 54.

Configuring Fibre Transport properties

NetBackup Fibre Transport properties control how your SAN clients use the Fibre Transport services for backups. NetBackup uses a hierarchy of properties to provide increasingly granular control of how your clients use NetBackup Fibre Transport.

See "About configuring Fibre Transport properties" on page 47.

To configure NetBackup FT properties

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Host Properties**.
2. Depending on which level of properties you want to configure, do one of the following:

To configure global FT properties	Select **Master Servers**.
To configure FT properties for a media server or servers	Select **Media Servers**.
To configure FT properties for a client or clients	Select **Clients**.

3. Select the host or hosts to configure, as follows:
   - To configure the properties on one host, double-click the name of the host in the right pane.
   - To configure properties for more than one host, select the hosts and then on the **Actions** menu select **Properties**.
4. In the host properties dialog box, click **Fibre Transport** in the left pane.
5. Configure the properties.

   See "Fibre Transport properties" on page 49.

Fibre Transport properties

NetBackup Fibre Transport properties control how your Fibre Transport media servers and SAN clients use the Fibre Transport service for backups and restores. The **Fibre Transport** properties apply to the host type that you select in the **NetBackup Administration Console**, as follows:

Table 5-7 Host types for Fibre Transport properties

Host type	Description
Master server	Global **Fibre Transport** properties that apply to all SAN clients.
Media server	The **Fibre Transport Maximum concurrent FT connections** property applies to the FT media server or servers that you selected in the **NetBackup Administration Console**.

Table 5-7 Host types for Fibre Transport properties *(continued)*

Host type	Description
Client	The **Fibre Transport** properties apply to the SAN client or clients that you selected in the **NetBackup Administration Console**. The default values for clients are the global property settings of the master server. Client properties override the global **Fibre Transport** properties.

Figure 5-1 Fibre Transport host properties for a master server

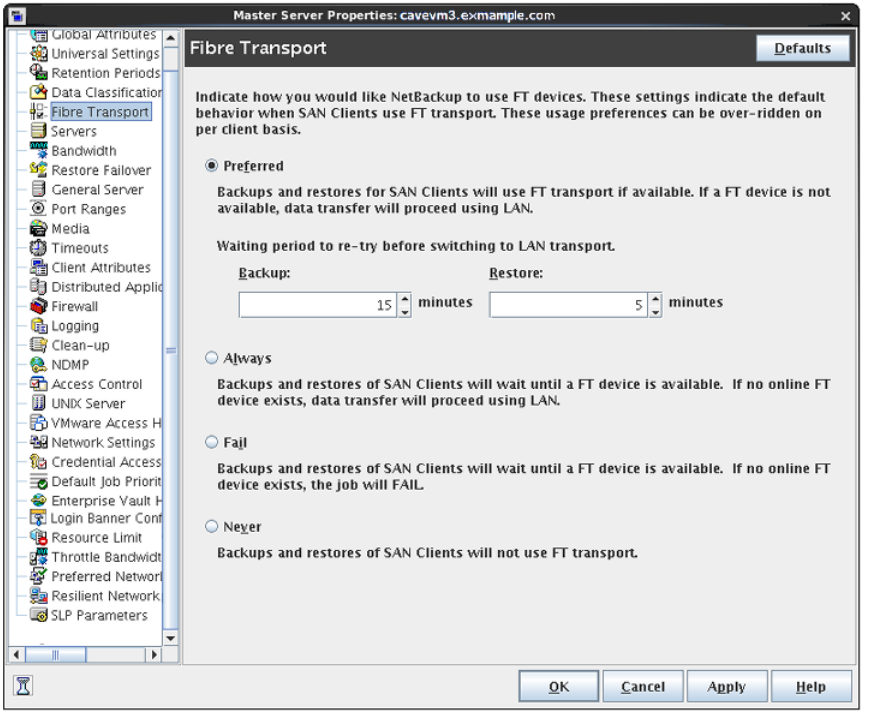


Table 5-8 describes the **Fibre Transport** properties. All properties are not available for all hosts. In this table, FT device is an HBA port on a Fibre Transport media server. The port carries the backup and restore traffic. A media server may have more than one FT device.

Table 5-8 Fibre Transport dialog box properties

Property	Description
Maximum concurrent FT connections	This property appears only when you select an FT media server or servers in the **NetBackup Administration Console**. This property specifies the number of FT connections to allow to the selected media server or media servers. A connection is equivalent to a job. NetBackup supports 644 buffers per media server for Fibre Transport. To determine the number of buffers that each connection uses, divide 644 by the value you enter. More buffers per connection equal better performance for each connection. If no value is set, NetBackup uses the following defaults: ■ For NetBackup Appliance model 5330 and later: 32 ■ For NetBackup Appliance model 5230 and later: 32 ■ For NetBackup Fibre Transport media servers: 8 times the number of fast HBA ports on the media server plus 4 times the number of slow HBA ports for. A fast port is 8 GB or faster, and a slow port is less than 8 GB. You can enter up to the following maximum connections for the media server or servers to use: ■ On a Linux FT media server host: 40. Symantec recommends that you use 32 or fewer connections concurrently on Linux. On Linux hosts, you can increase that maximum by setting a NetBackup touch file, `NUMBER_DATA_BUFFERS_FT`. See "About Linux concurrent FT connections" on page 52. ■ For NetBackup Appliance model 5330 and later: 40. ■ For NetBackup Appliance model 5230 and later: 40. ■ On a Solaris FT media server host: 64.
Use defaults from the master server configuration	This property appears only when you select a client or client in the **NetBackup Administration Console**. This property specifies that the client follow the properties as they are configured on the master server.
Preferred	The **Preferred** property specifies to use an FT device if one is available within the configured wait period in minutes. If an FT device is not available after the wait period elapses, NetBackup uses a LAN connection for the operation. If you select this option, also specify the wait period for backups and for restores. For the global property that is specified on the master server, the default is **Preferred**.

Table 5-8 Fibre Transport dialog box properties *(continued)*

Property	Description
Always	The **Always** property specifies that NetBackup should always use an FT device for backups and restores of SAN clients. NetBackup waits until an FT device is available before it begins the operation. However, an FT device must be online and up. If not, NetBackup uses the LAN. An FT device may be unavailable because none are active, none have been configured, or the SAN Client license expired.
Fail	The **Fail** property specifies that NetBackup should fail the job if an FT device is not online and up. If the FT devices are online but busy, NetBackup waits until a device is available and assigns the next job to the device. An FT device may be unavailable because none are active, none have been configured, or the SAN Client license expired.
Never	The **Never** property specifies that NetBackup should never use an FT pipe for backups and restores of SAN clients. NetBackup uses a LAN connection for the backups and restores. If you specify **Never** for the master server, Fibre Transport is disabled in the NetBackup environment. If you select **Never**, you can configure FT usage on a per-client basis. If you specify **Never** for a media server, Fibre Transport is disabled for the media server. If you specify **Never** for a SAN client, Fibre Transport is disabled for the client.

See "Configuring Fibre Transport properties" on page 48.

NetBackup provides one finer level of granularity for Fibre Transport. SAN client usage preferences override the FT properties that you configure through **Host Properties**.

See "About SAN client usage preferences" on page 53.

About Linux concurrent FT connections

NetBackup uses the **Maximum concurrent FT connections Fibre Transport** host property to configure the number of concurrent connections to a Fibre Transport media server, up to the total that is allowed per host.

See "Fibre Transport properties" on page 49.

If the total number of concurrent connections on Linux is too low for your purposes, you can increase the total number of concurrent connections. The consequence is that each client backup or restore job uses fewer buffers, which means that each job is slower because of fewer buffers. To increase the number of concurrent

connections, reduce the number of buffers per connection. To do so, create the following file and include one of the supported values in the file:

`/usr/openv/netbackup/db/config/NUMBER_DATA_BUFFERS_FT`

Table 5-9 shows the values that NetBackup supports for the `NUMBER_DATA_BUFFERS_FT` file. NetBackup supports 644 buffers per media server for Fibre Transport.

Table 5-9 Supported values for buffers per FT connection

NUMBER_DATA_BUFFERS_FT	Total concurrent connections: NetBackup 5230 and 5330 and later appliances	Total concurrent connections: Linux FT media server
16	40	40
12	53	53
10	64	64

If you want, you then can limit the number of connections for a media server or media servers by using the **Maximum concurrent FT connections** of the **Fibre Transport** host properties.

About SAN client usage preferences

SAN client usage preferences let you configure how a SAN client uses NetBackup Fibre Transport for backups.

See "Configuring SAN client usage preferences" on page 53.

The usage preferences override the FT transport properties.

See "About configuring Fibre Transport properties" on page 47.

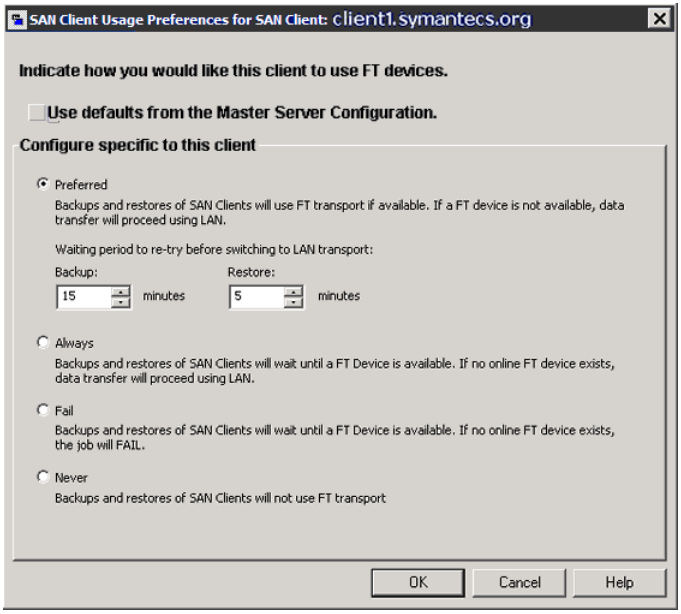
Configuring SAN client usage preferences

SAN client usage preferences let you configure how a specific client uses NetBackup Fibre Transport for backups.

SAN client usage preferences override the NetBackup Fibre Transport properties.

To configure SAN client usage preferences by using the Devices node

1. In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management > Devices**.
2. Select **SAN Clients**.
3. Select a client or clients in the right pane.
4. On the **Actions** menu, select **SAN Client Usage Preferences**.
5. In the **SAN Client Usage Preferences** dialog box, configure the properties.



See "SAN client usage preferences" on page 54.

SAN client usage preferences

The following table describes the Fibre Transport usage preferences for SAN clients.

Table 5-10 SAN client Fibre Transport usage preferences

Property	Description
Use defaults from the master server configuration	This property specifies that the client follow the properties as they are configured on the master server.

Table 5-10 SAN client Fibre Transport usage preferences *(continued)*

Property	Description
Preferred	The **Preferred** property specifies to use an FT device if one is available within the configured wait period in minutes. If an FT device is not available after the wait period elapses, NetBackup uses a LAN connection for the operation. If you select this option, also specify the wait period for backups and for restores. For the global property that is specified on the master server, the default is **Preferred**.
Always	The **Always** property specifies that NetBackup should always use an FT device for backups and restores of SAN clients. NetBackup waits until an FT device is available before it begins the operation. However, an FT device must be online and up. If not, NetBackup uses the LAN. An FT device may not exist because none is active, none have been configured, or the SAN Client license expired.
Fail	The **Fail** property specifies that NetBackup should fail the job if an FT device is not online and up. If the FT devices are online but busy, NetBackup waits until a device is available and assigns the next job to the device. An FT device may not exist because none is active, none have been configured, or the SAN Client license expired.
Never	The **Never** property specifies that NetBackup should never use an FT pipe for backups and restores of SAN clients. NetBackup uses a LAN connection for the backups and restores. If you specify **Never** for the master server, Fibre Transport is disabled in the NetBackup environment. If you select **Never**, you can configure FT usage on a per-client basis. If you specify **Never** for a media server, Fibre Transport is disabled for the media server. If you specify **Never** for a SAN client, Fibre Transport is disabled for the client.

Chapter 6

Managing SAN clients and Fibre Transport

This chapter includes the following topics:

Enabling or disabling the Fibre Transport services

You can enable or disable the FT services on NetBackup FT media servers.

The following are the services that compose the FT server:

- The `nbftsrvr` service manages the server side of the FT pipe.
- The `nbfdrv64` service controls the target mode drivers on the media server.

The `nbftsrvr` service starts the `nbfdrv64` service. If you stop one, the other stops. If one ends abnormally, the other stops.

These services do not appear in the **NetBackup Activity Monitor**; they do appear in the operating system process displays.

Warning: Do not use the UNIX `kill -9` command and option to stop the `nbfdrv64` process. It does not allow the process to stop gracefully, and the SAN clients cannot detect the FT devices when the `nbfdrv64` process dies. You then may have to restart the client systems so they detect the FT devices again (after you restart `nbfdrv64`).

To enable or disable FT services

1. In the **NetBackup Administration Console** on the master server, in the left pane, expand **Media and Device Management > Devices > Media Server**.
2. Select an FT media server in the right pane.
3. Click either **Actions** > **Enable FT Services** or **Actions > Disable FT Services**.

Rescanning for Fibre Transport devices from a SAN client

A rescan operation tries to find new FT devices from the client. If the scan detects new FT devices, NetBackup adds them to the EMM database. A rescan operation is a time- and compute-intensive operation. It may not discover new devices (especially if the client system requires a restart and you do not restart it).

Depending on the operating system capabilities and the HBA driver and its settings, the scan may search for new Fibre Channel devices.

To rescan SAN clients

1. On Microsoft Windows clients, use the Windows Device Manager to scan for hardware changes.
2. In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management > Devices > SAN Clients**.
3. Select a client in the right pane.
4. Click **Action** > **Rescan SAN Client FT Devices**.
5. In the **Rescan SAN Client** dialog box, monitor the following status of the operation:
   - Initiated
   - Client system must be restarted
   - Failure
6. If required, restart the client system.

Viewing SAN Client Fibre Transport job details

The **NetBackup Administration Console** Activity Monitor **Jobs** tab displays all of the jobs that are in progress or have been completed.

The **Transport** column in the **Jobs** tab window shows the type of transport between the SAN client and the NetBackup media server: FT for Fibre Transport or blank for inactive or for a LAN.

The **Detailed Status** tab of the **Job Details** dialog shows more detailed information about the job, including the following:

- A **Transport Type** field in the header area shows the same information as the **Transport** column in the **Jobs** tab.
- Messages in the **Status** window show the status of jobs that use FT transport, as follows:
  - Queuing for FT transport
  - Allocated FT transport
  - Opening FT connection
  - Closing FT connection

See "Viewing Fibre Transport traffic" on page 58.

To view job details

- Double-click the job in the **Jobs** tab.

  The **Job Details** dialog appears that contains detailed job information on a **Job Overview** tab and a **Detailed Status** tab.

Viewing Fibre Transport traffic

You can view the current activity between FT media servers and SAN clients. The following two views are available:

FT media server view	The media server view shows all of the inbound backup (and outbound restore) traffic for a selected FT media server. Use this view to determine which SAN clients can send data to and receive data from the selected media server. See "To view FT activity from the media server perspective" on page 59.

SAN Client view	The SAN client view shows all of the outbound backup (and inbound restore) traffic for a selected client. Use this view to determine which FT media servers can send data to and receive data from the selected client. See "To view FT activity from the client perspective" on page 59.

See "Viewing SAN Client Fibre Transport job details" on page 58.

To view FT activity from the media server perspective

1. In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management > Devices > Media Server**.
2. Select an FT media server in the right pane.
3. Click **Actions > View FT Connections**.

   The **Media Server Fibre Transport View** dialog box shows the connection activity for the media server.

To view FT activity from the client perspective

1. In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management > Devices > SAN Clients**.
2. Select a client in the right pane.
3. Click **Actions > View FT Connections**.

   The **SAN Client Fibre Transport View** dialog box shows the connection activity for the client.

Adding a SAN client

If you configure a SAN client and it does not appear as a SAN client in your NetBackup environment, you can add the client. To do so, use the **NetBackup Device Configuration Wizard** or the **NetBackup Administration Console**.

The SAN client must be configured correctly and the SAN client FT service must be active.

To add a SAN client by using the wizard

1. In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management**.
2. In the right pane, click **Configure Storage Devices**.

3 Follow the wizard screens.

4 If the SAN client does not appear on the SAN clients screen, click **Add** to add it manually.

To add a SAN client by using the Administration Console

1 In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Devices > SAN Clients**.

2 Click **Actions > New > New SAN Client**.

3 In the **New SAN Client** dialog box, enter the name of the client and click **OK**.

NetBackup queries the client and adds it to the **SAN Clients** list in the **Administration Console** window.

Deleting a SAN client

Use the following procedure to delete a SAN client from your NetBackup configuration. The SAN client remains a NetBackup client, but it no longer functions as a SAN client.

To delete a SAN client

1 Disable the SAN client services.

See "Disabling a SAN client" on page 61.

2 In the **NetBackup Administration Console**, in the left pane, select **Media and Device Management > Devices > SAN Clients**.

3 Select a client in the right pane.

4 Click **Edit** > **Delete**.

Chapter 7

Disabling SAN Client and Fibre Transport

This chapter includes the following topics:

About disabling SAN Client and Fibre Transport

You cannot uninstall the SAN Client and Fibre Transport components. However, you can disable the SAN clients and the FT media servers.

See “Disabling a SAN client” on page 61.

See “Disabling a Fibre Transport media server” on page 62.

Disabling a SAN client

You can disable a SAN client. If you do, the client cannot backup over the SAN to an FT media server.

See “About disabling SAN Client and Fibre Transport” on page 61.

After you disable a SAN client, you can remove it from your NetBackup environment.

See “Deleting a SAN client” on page 60.

To disable the NetBackup SAN client service on UNIX

1. To stop the service, run the following command on the client:

   ```
   /usr/openv/netbackup/bin/nbftclnt -terminate
   ```

2. To configure the host so it does not start the SAN client service after a computer restart, run the following command:

   ```
   /usr/openv/netbackup/bin/bpclntcmd -sanclient 0
   ```

To disable the NetBackup SAN client service on Windows

1. Use Windows Computer Management to stop the NetBackup SAN Client Service.
2. To configure the host so it does not start the SAN client service after a restart, run the following command:

   install_path\NetBackup\bin\bpclntcmd.exe -sanclient 0

Disabling a Fibre Transport media server

You can disable an FT media server and remove the operating system FT startup scripts from the media server. The process also removes the `nbhba` driver and exits `nbhba` mode. The media server then does not support NetBackup Fibre Transport.

See "About disabling SAN Client and Fibre Transport" on page 61.

Warning: On Solaris systems, `/etc/driver_aliases` file entries may remain after you remove the FT services and the `nbhba` driver. The entries are in the form of qla2300 "pci1077,xxx" or qla2300 "pciex1077,xxx. The entries are harmless; however, if you attempt to remove them, the system may not boot. Sun Microsystems recommends that you do not edit the `/etc/driver_aliases` file.

To disable an FT media server and remove drivers

1. On the FT media server, run the following script:

   ```
   /usr/openv/netbackup/bin/admincmd/nbftsrv_config -d
   ```

2. Verify that the following startup scripts were removed:

   On Linux systems, the following are the scripts:

   ```
   /etc/rc.d/rc2.d/S21nbftserver
   /etc/rc.d/rc3.d/S21nbftserver
   /etc/rc.d/rc5.d/S21nbftserver
   /etc/rc.d/rc0.d/K03nbftserver
   /etc/rc.d/rc6.d/K03nbftserver
   /lib/modules/ 2.6.*smp/kernel/drivers/misc/ql2300_stub.ko
   /lib/modules/ 2.6.*smp/kernel/drivers/misc/windrvr6.ko
   ```

   On Solaris systems, the following are the scripts:

   ```
   /etc/rc2.d/S21nbftserver
   /etc/rc0.d/K03nbftserver
   /usr/kernel/drv/windrvr6.conf
   /usr/kernel/drv/sparcv9/windrvr6
   /usr/kernel/drv/sparcv9/ql2300_stub
   ```

3. If the startup scripts were not removed, delete them manually.

4. Run the following script:

   ```
   /usr/openv/netbackup/bin/admincmd/nbftconfig -ds
   ft_server_host_name
   ```

Chapter 8

Troubleshooting SAN Client and Fibre Transport

This chapter includes the following topics:

About troubleshooting SAN Client and Fibre Transport

SAN Client and Fibre Transport troubleshooting information is available.

See "SAN Client troubleshooting tech note" on page 65.

See "Viewing Fibre Transport logs" on page 65.

See "Stopping and starting Fibre Transport services" on page 69.

See "Backups failover to LAN even though Fibre Transport devices available " on page 70.

See "SAN client service does not start" on page 71.

See "SAN client Fibre Transport service validation" on page 72.

See "SAN client does not select Fibre Transport" on page 73.

See "Media server Fibre Transport device is offline" on page 73.

See "No Fibre Transport devices discovered" on page 74.

SAN Client troubleshooting tech note

More troubleshooting information about SAN clients and Fibre Transport is available on the Symantec Enterprise Support Web site in the following Tech Note:

http://www.symantec.com/docs/TECH51454

The Tech Note contents are updated when new information is available. The Tech Note may contain more current information than this guide.

Viewing Fibre Transport logs

You can monitor Fibre Transport activity and status by viewing the log messages that the FT processes generate. Veritas unified log (VxUL) files use a standardized name and file format for log files. An originator ID identifies the process that writes the log messages.

Table 8-1 shows the VxUL originator IDs of the processes that log information about FT activity.

Table 8-1 Fibre Transport originator IDs

Originator ID	FT processes that use the ID
199	`nbftsrvr` and `nbfdrv64`. The media server Fibre Transport services.
200	`nbftclnt`. The client Fibre Transport service.
201	The FT Service Manager. Runs in the Enterprise Media Manager service.

To view and manage VxUL log files, you must use NetBackup log commands.

See "About unified logging" on page 66.

Configure the amount of information that is collected and its retention length on the NetBackup master server in the **Logging** properties and **Clean-up** properties.

Information about how to configure logging and clean-up properties is available in the *NetBackup Administrator's Guide, Volume I*:

http://www.symantec.com/docs/DOC5332

About unified logging

Unified logging and legacy logging are the two forms of debug logging used in NetBackup. Unified logging creates log file names and messages in a standardized format. All NetBackup processes use either unified logging or legacy logging.

Unlike the files that are written in legacy logging, unified logging files cannot be easily viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file. Only the `vxlogview` command can assemble and display the log information correctly.

Server processes and client processes use unified logging.

Unlike legacy logging, unified logging does not require that you create logging subdirectories. Log files for originator IDs are written to a subdirectory with the name specified in the log configuration file. All unified logs are written to subdirectories in the following directory:

Windows	*install_path*\NetBackup\logs
UNIX	/usr/openv/logs

You can access logging controls in the **NetBackup Administration Console**. In the left pane, expand **NetBackup Management > Host Properties > Master Servers** or **Media Servers**. Double-click the server you want to change. In the left pane of the dialog box, click **Logging**.

You can also manage unified logging by using the following commands:

`vxlogcfg`	Modifies the unified logging configuration settings.
`vxlogmgr`	Manages the log files that the products that support unified logging generate.
`vxlogview`	Displays the logs that unified logging generates. See "Examples of using vxlogview to view unified logs" on page 67.

See the *NetBackup Commands Reference Guide* for a complete description about these commands. The guide is available through the following URL:

http://www.symantec.com/docs/DOC5332

These commands are located in the following directory:

Windows	*install_path*\NetBackup\bin
UNIX	/usr/openv/netbackup/bin

About using the vxlogview command to view unified logs

Use the `vxlogview` command to view the logs that unified logging creates. These logs are stored in the following directory.

UNIX	/usr/openv/logs
Windows	*install_path*\NetBackup\logs

Unlike the files that are written in legacy logging, unified logging files cannot be easily viewed with a text editor. The unified logging files are in binary format, and some of the information is contained in an associated resource file. Only the `vxlogview` command can assemble and display the log information correctly.

You can use `vxlogview` to view NetBackup log files as well as PBX log files.

To view PBX logs using the `vxlogview` command, do the following:

- Ensure that you are an authorized user. For UNIX and Linux, you must have root privileges. For Windows, you must have administrator privileges.
- To specify the PBX product ID. enter `-p 50936` as a parameter on the `vxlogview` command line.

`vxlogview` searches all the files, which can be a slow process. Refer to the following topic for an example of how to display results faster by restricting the search to the files of a specific process.

Examples of using vxlogview to view unified logs

The following examples demonstrate how to use the `vxlogview` command to view unified logs.

Table 8-2 Example uses of the vxlogview command

Item	Example
Display all the attributes of the log messages	`vxlogview -p 51216 -d all`
Display specific attributes of the log messages	Display the log messages for NetBackup (51216) that show only the date, time, message type, and message text: `vxlogview --prodid 51216 --display D,T,m,x`
Display the latest log messages	Display the log messages for originator 116 (`nbpem`) that were issued during the last 20 minutes. Note that you can specify `-o nbpem` instead of `-o 116`: `# vxlogview -o 116 -t 00:20:00`
Display the log messages from a specific time period	Display the log messages for `nbpem` that were issued during the specified time period: `# vxlogview -o nbpem -b "05/03/05 06:51:48 AM" -e "05/03/05 06:52:48 AM"`
Display results faster	You can use the `-i` option to specify an originator for a process: `# vxlogview -i nbpem` The `vxlogview -i` option searches only the log files that the specified process (`nbpem`) creates. By limiting the log files that it has to search, `vxlogview` returns a result faster. By comparison, the `vxlogview -o` option searches all unified log files for the messages that the specified process has logged. **Note:** If you use the `-i` option with a process that is not a service, `vxlogview` returns the message "No log files found." A process that is not a service has no originator ID in the file name. In this case, use the `-o` option instead of the `-i` option. The -i option displays entries for all OIDs that are part of that process including libraries (137, 156, 309, etc.).

Table 8-2 Example uses of the vxlogview command *(continued)*

Item	Example
Search for a job ID	You can search the logs for a particular job ID: `# vxlogview -i nbpem | grep "jobid=job_ID"` The `jobid=` search key should contain no spaces and must be lowercase. When searching for a job ID, you can use any `vxlogview` command option. This example uses the `-i` option with the name of the process (`nbpem`). The command returns only the log entries that contain the job ID. It misses related entries for the job that do not explicitly contain the jobid=*job_ID*.

See the *NetBackup Commands Reference Guide* for a complete description of the `vxlogview` command. The guide is available through the following URL:

http://www.symantec.com/docs/DOC5332

Stopping and starting Fibre Transport services

Fibre Transport services run on both the FT media servers and SAN clients.

The following are the FT services that run on media servers:

- The `nbftsrvr` service manages the server side of the FT pipe.
- The `nbfdrv64` service controls the target mode drivers on the media server.

The `nbftsrvr` service starts the `nbfdrv64` service. If you stop one, the other stops. If one ends abnormally, the other stops.

The `nbftclnt` FT service runs on SAN clients:

These services do not appear in the NetBackup Activity Monitor; they do appear in the operating system process displays.

In normal operation, you should not have to start or stop the services. A Symantec support engineer may direct you to stop and restart services for troubleshooting purposes.

See "Enabling or disabling the Fibre Transport services" on page 56.

Alternatively, you can use the UNIX `kill` command without the `-9` option to stop the services. The NetBackup `bp.kill_all` command stops the FT services, but it stops all other NetBackup services also.

Warning: Do not use the UNIX `kill -9` command and option to stop the nbfdrv64 process. It does not allow the process to stop gracefully, and the SAN clients cannot detect the FT devices when the nbfdrv64 process dies. You then may have to reboot the client systems so they detect the FT devices again (after you restart nbfdrv64).

The NetBackup `bp.start_all` command starts all NetBackup services, including the FT services.

Backups failover to LAN even though Fibre Transport devices available

If a NetBackup FT media server has multiple network interfaces for VLANs, backups may failover to LAN transport if the NetBackup host name order is configured incorrectly.

See "About Fibre Transport media servers and VLANs" on page 33.

For all of the hosts that participate in the backups, examine their **Additional Servers** lists on their **NetBackup Administration Console** host properties **Servers** pages. Verify that the FT server's primary host name appears before any other interface names for that FT media server host in. If it does not, fix the incorrect host name order as described in the following table.

Table 8-3 How to fix an incorrect host name order in NetBackup

Task	Procedure
Stop the FT services on the media server	See "Enabling or disabling the Fibre Transport services" on page 56.
Delete the FT server from the NetBackup EMM database	Use the following NetBackup command to delete the host from the NetBackup EMM database as an FT media server: `nbftconfig -deleteserver -Me` *`hostname`* The host remains in the EMM database as a NetBackup media server.

Table 8-3 How to fix an incorrect host name order in NetBackup *(continued)*

Task	Procedure
Re-order the **Additional Servers** list on each host	If necessary, delete all of the network interface names of the FT media server from the **Additional Servers** list. Then, add the primary host name first and then the remainder of the host names in any order. The **Additional Servers** list appears in the host properties **Servers** page for that host. See the *NetBackup Administrator's Guide, Volume I*: http://www.symantec.com/docs/DOC5332
Start the FT services on the media server	See "Enabling or disabling the Fibre Transport services" on page 56.
Scan for FT devices from each SAN client	When the FT media server is discovered during the rescan operation, NetBackup adds it to the EMM database as an FT media server. See "Rescanning for Fibre Transport devices from a SAN client" on page 57.

Kernel warning messages when Symantec modules load

For Linux operating systems, warning messages similar to the following may appear in the console or the system log when Symantec modules are loaded into the kernel:

```
kernel: ql2300_stub: module license 'Proprietary. Send bug
reports to support@symantec.com' taints kernel.
kernel: ql2300_stub: Version: XXn
kernel: ql2300_stub: $Revision: n.nn
```

The messages appear because the Symantec modules are proprietary. You can ignore them.

SAN client service does not start

The `nbftclnt` service is the SAN Client service that runs on clients, If it does not start on UNIX or Linux systems, one possible cause may be the NetBackup configuration file. The following is the pathname of the file:

```
/usr/openv/netbackup/bp.conf
```

If the client host name is listed as a `SERVER`, the `nbftclnt` service does not start. If a `SERVER` entry exists for the client, remove the entry and then start the client service.

The client host name should be listed as `CLIENT_NAME` only.

SAN client Fibre Transport service validation

The SAN Client Fibre Transport Service (nbftclnt) validates the client system's kernel and driver stack when it starts and during device discovery. Validation verifies that the kernel and the drivers are at supported levels.

If validation succeeds, the SAN client supports FT pipe transfers; FT pipe transfer can occur. If validation fails, FT pipe transfer cannot occur.

To manage the validation failure, the following occurs:

- The SAN Client Fibre Transport Service writes check driver messages in its log file.
- NetBackup sets the FT device status to offline for all FT target devices in the client's SAN zone. (For other clients in the zone that pass the validation, the FT devices are online.)

To see the FT device status from the client, select the client in the **Media and Device Management > Devices > SAN Clients** window in the **NetBackup Administration Console**.

The check driver messages in the nbftclnt log file are similar to the following:

```
VerifyCheckConditions:failed on <OS Device Name> - check driver
VerifyCheckConditions:failed on <OS Device Name>; <System Error
Message>
```

The following describes the variables in the messages:

- *OS Device Name* is the device name the SAN Client uses to open the OS device driver.
- *System Error Message* can be any OS-dependent system error message for a failure that is associated with the request.

See "Viewing Fibre Transport logs" on page 65.

If validation fails, install the correct operating system version, operating system patches, or driver version.

For supported kernel and driver levels, see the *NetBackup Release Notes*.

SAN client does not select Fibre Transport

If either of the following are true, a SAN client may not be able to select Fibre Transport during a backup or restore operation:

- The FT media server host operating system `domainname` command returns fully qualified domain names and NetBackup is configured to use short names.
- The FT media server host operating system `domainname` command fails because of: DNS, NIS, or network problems and NetBackup is configured to use fully qualified domain names.

If so, the backup or restore may fail or it may occur over the LAN rather than the SAN.

To work around this problem, add an alias for the FT media server to the EMM database.

The following are the command syntaxes:

- To add a short name alias:

```
nbemmcmd -machinealias -addalias -alias shortservername
-machinename servername.fully.qualified -machinetype media
```

- To add a fully qualified domain name alias:

```
nbemmcmd -machinealias -addalias -alias
servername.fully.qualified -machinename shortservername
-machinetype media
```

Media server Fibre Transport device is offline

If NetBackup shows that a media server FT device is offline, the selected SAN client cannot detect the target mode driver on that media server. FT device status appears in the Media and Device Management > Devices > SAN Clients window of the NetBackup Administration Console. (An FT device represents the HBA target mode driver on a media server.)

An FT device may be offline because of the following:

- The nbfdrv64 service on a media server is down. The `nbfdrv64` service manages the target mode drivers; if it is down, the FT device is not available.
- The physical connections between the SAN client and the SAN switch fail or were changed.

- SAN zoning changes removed either the media server or the SAN client from the zone.
- The SAN client failed the FT service validation.
  See “SAN client Fibre Transport service validation” on page 72.

If all media server FT devices for a client are offline, troubleshoot in the following order:

- Verify that the SAN client FT service validation passes.
- Verify that the physical connections from the SAN client to the SAN switch are correct.
- Verify that the SAN zones are correct.
- Verify that the `nbfdrv64` service is active on each media server.

To determine if the `nbfdrv64` service is down, use the operating system process status command to examine the processes on the media server. Both `nbftsrvr` and `nbfdrv64` should be active.

See “Stopping and starting Fibre Transport services” on page 69.

If the services do not start, examine the log files for those services to determine why they do not start.

See “Viewing Fibre Transport logs” on page 65.

No Fibre Transport devices discovered

If a "No FT devices discovered" message appears in the NetBackup logs on the SAN client, the pass-through driver may not be configured on the SAN client.

For information about how to configure pass-through drivers, see the *NetBackup Device Configuration Guide*, available at the following URL:

http://www.symantec.com/docs/DOC5332

Index

T

U

V

W