

NetBackup™ SAN Client and Fibre Transport Guide

UNIX, Windows, Linux

Release 11.1

NetBackup™ SAN Client and Fibre Transport Guide

Last updated: 2025-11-24

Legal Notice

Copyright © 2025 Cohesity, Inc. All rights reserved.

Cohesity, Veritas, the Cohesity Logo, Veritas Logo, Veritas Alta, Cohesity Alta, and NetBackup are trademarks or registered trademarks of Cohesity, Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Cohesity is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Cohesity product or available at:

<https://www.veritas.com/about/legal/license-agreements>

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

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

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

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Cohesity account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Cohesity website.

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Introducing SAN Client and Fibre Transport	8
	About NetBackup SAN Client and Fibre Transport	8
	About Fibre Transport	9
	About Fibre Transport media servers	10
	About SAN clients	10
	About the Fibre Transport Service Manager	11
	Supported systems and peripherals	11
Chapter 2	Planning your deployment	12
	Planning your SAN Client deployment	12
	SAN Client operational notes	13
	About SAN Client storage destinations	13
	About SAN Client disk storage destinations	14
	About SAN Client tape storage destinations	14
	How to choose SAN Client and Fibre Transport hosts	15
	About NetBackup SAN Client support for agents	15
	About NetBackup SAN Client support for clustering	16
	About NetBackup SAN Client support for Windows Hyper-V Server	16
	About NetBackup SAN Client unsupported restores	17
	About Fibre Transport throughput	17
	Converting a SAN media server to a SAN client	18
Chapter 3	Preparing the SAN	20
	Preparing the SAN	20
	About zoning the SAN for Fibre Transport	21
	About zoning the SAN for Fibre Transport for a 16-gigabit target mode HBA support	23
	About HBAs for SAN clients and Fibre Transport media servers	25
	About the 16-gigabit target mode HBAs for SAN clients and Fibre Transport media servers	26
	When selecting the HBA ports for SAN Client	27
	About supported SAN configurations for SAN Client	27

Chapter 4	Licensing SAN Client and Fibre Transport	29
	About SAN Client installation	29
	About the SAN Client license	29
	When upgrading SAN Client and Fibre Transport	29
Chapter 5	Configuring SAN Client and Fibre Transport	31
	Overview of configuring SAN Client and Fibre Transport	31
	Configuring a Fibre Transport media server	32
	About the target mode driver	33
	About nbhba mode and the ql2300_stub driver	34
	About FC attached devices	34
	How to identify the HBA ports	35
	About HBA port detection on Solaris	36
	About Fibre Transport media servers and VLANs	36
	Start nbhba mode	37
	Mark the Fibre Transport media server HBA ports	38
	Configure the media server Fibre Transport services	41
	Configure the media server Fibre Transport services for a 16-gigabit target mode HBA support	45
	Display the FTMS state for a 16-gigabit target mode HBA support	51
	Identify the HBA ports for a 16-gigabit target mode HBA support	51
	Configuring SAN clients	52
	About configuring firewalls for SAN clients	52
	SAN client driver requirements	52
	Configure the SAN Client Fibre Transport service	53
	Configuring SAN clients in a cluster	55
	Register a SAN client cluster virtual name	56
	Setting NetBackup configuration options by using the command line	57
	About configuring Fibre Transport properties	58
	Configure Fibre Transport properties	59
	Fibre Transport properties	60
	About Linux concurrent FT connections	63
	Configure SAN client usage preferences	64
	SAN client usage preferences	64

Chapter 6	Managing SAN clients and Fibre Transport	66
	Enable or disable the Fibre Transport services	66
	Enable or disable the Fibre Transport services for a 16-gigabit target mode HBA support	67
	Rescan for Fibre Transport devices from a SAN client	67
	View the SAN client Fibre Transport job details	68
	View the Fibre Transport traffic	69
	Delete a SAN client	70
Chapter 7	Disabling SAN Client and Fibre Transport	71
	Disable a SAN client	71
	Disable a Fibre Transport media server	72
	Disable a Fibre Transport media server for a 16-gigabit target mode HBA support	73
Chapter 8	Troubleshooting SAN Client and Fibre Transport	75
	About troubleshooting SAN Client and Fibre Transport	76
	SAN Client troubleshooting tech note	76
	View the Fibre Transport logs	76
	About unified logging	77
	About using the <code>vxlogview</code> command to view unified logs	78
	Examples of using <code>vxlogview</code> to view unified logs	80
	Stop and start the Fibre Transport services	81
	Stop and start the Fibre Transport services for a 16-gigabit target mode HBA support	82
	Backups failover to LAN even though Fibre Transport devices available	83
	Kernel warning messages when Cohesity modules load	84
	SAN client service does not start	84
	SAN Client Fibre Transport Service validation	84
	SAN client does not select Fibre Transport	85
	Media server Fibre Transport device is not active	86
	No Fibre Transport devices discovered	87
Appendix A	AIX specific configuration details	88
	AIX Reference Information	88
	Before you begin configuring NetBackup on AIX	88
	About AIX persistent naming support	89
	About configuring robotic control device files in AIX	89

About device files for SAN Clients on AIX	89
About non-QIC tape drives on AIX	90
About no rewind device files on AIX	90
Create AIX no rewind device files for tape drives	91
Disable the AIX dynamic tracking	92

Introducing SAN Client and Fibre Transport

This chapter includes the following topics:

- [About NetBackup SAN Client and Fibre Transport](#)
- [About Fibre Transport](#)
- [About Fibre Transport media servers](#)
- [About SAN clients](#)
- [About the Fibre Transport Service Manager](#)
- [Supported systems and peripherals](#)

About NetBackup SAN Client and Fibre Transport

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

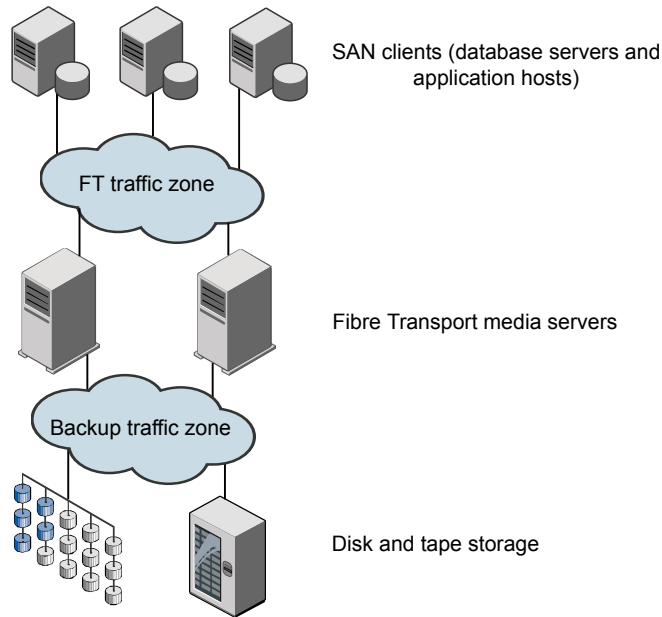
A SAN client is a special NetBackup client that can back up large amounts of data rapidly over a SAN connection rather than a LAN. For example, a database host can benefit from high-speed backups and restores. Fibre Transport is the name of the NetBackup high-speed data transport method that is part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

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

For a NetBackup 52xx or 53xx appliance, Fibre Transport also provides high-speed traffic to a NetBackup 5000 series appliance that supports Fibre Transport. The 5000 series appliance functions as the storage host for SAN client backups.

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 a license that activates the SAN Client feature

See [“Configuring a Fibre Transport media server”](#) on page 32.

See [“Fibre Transport properties”](#) on page 60.

See [“About NetBackup SAN Client and Fibre Transport”](#) on page 8.

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.

<http://www.veritas.com/docs/DOC5332>

See [“Configuring SAN clients”](#) on page 52.

See [“About configuring firewalls for SAN clients”](#) on page 52.

See [“SAN client driver requirements”](#) on page 52.

See [“Configure the SAN Client Fibre Transport service”](#) on page 53.

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.

Supported systems and peripherals

For limitations and operational notes, see the [NetBackup Release Notes](#). For information about supported systems and peripherals, see the [Services and Operations Readiness Tools \(SORT\)](#) site.

Planning your deployment

This chapter includes the following topics:

- [Planning your SAN Client deployment](#)
- [SAN Client operational notes](#)
- [About SAN Client storage destinations](#)
- [How to choose SAN Client and Fibre Transport hosts](#)
- [About NetBackup SAN Client support for agents](#)
- [About NetBackup SAN Client support for clustering](#)
- [About NetBackup SAN Client support for Windows Hyper-V Server](#)
- [About NetBackup SAN Client unsupported restores](#)
- [About Fibre Transport throughput](#)
- [Converting a SAN media server to a SAN client](#)

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 the operational notes	See " SAN Client operational notes " on page 13.

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 13.
Step 3	Determine the hosts to use	See “How to choose SAN Client and Fibre Transport hosts” on page 15.
Step 4	Prepare the SAN	See “Preparing the SAN” on page 20.
Step 5	License SAN Client	See “About the SAN Client license” on page 29.
Step 6	Read about NetBackup agents	See “About NetBackup SAN Client support for agents” on page 15.
Step 7	Read about SAN Client and Hyper-V	See “About NetBackup SAN Client support for Windows Hyper-V Server” on page 16.
Step 8	Configure SAN Client and Fibre Transport	See “Overview of configuring SAN Client and Fibre Transport” on page 31.
Step 9	Convert a SAN media server to a SAN Client	See “Converting a SAN media server to a SAN client” on page 18.

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.veritas.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 feature 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 primary 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).

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 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 primary server.

See “[Configuring SAN clients in a cluster](#)” on page 55.

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 52.

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.veritas.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 17.

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:

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 16.

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: <ul style="list-style-type: none"> ■ In the NetBackup web UI, click Storage > Media servers. ■ Select the host. ■ Select Delete device host.
Step 2	Uninstall the SAN media server software	See the NetBackup Installation Guide .
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 20.
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 20.
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 .
Step 6	Configure the FT media servers	See “Overview of configuring SAN Client and Fibre Transport” on page 31.
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 .

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

Step	Task	Instructions
Step 8	Configure the SAN client	See "Overview of configuring SAN Client and Fibre Transport" on page 31.
Step 9	Configure alternate server restore	<p>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.</p> <p>See Media host override setting in the General server properties of the primary server Host properties.</p> <p>After all of the images that were associated with the SAN media server expire, you can unconfigure the alternate server restore.</p>

Preparing the SAN

This chapter includes the following topics:

- [Preparing the SAN](#)
- [About zoning the SAN for Fibre Transport](#)
- [About zoning the SAN for Fibre Transport for a 16-gigabit target mode HBA support](#)
- [About HBAs for SAN clients and Fibre Transport media servers](#)
- [About the 16-gigabit target mode HBAs for SAN clients and Fibre Transport media servers](#)
- [When selecting the HBA ports for SAN Client](#)
- [About supported SAN configurations for SAN Client](#)

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 21.
Step 2	Install HBAs	See “About HBAs for SAN clients and Fibre Transport media servers” on page 25.
Step 3	Select HBA ports	See “When selecting the HBA ports for SAN Client” on page 27.

Table 3-1 SAN preparation overview (*continued*)

Step	Procedure	Section
Step 4	Connect the fiber	See “About supported SAN configurations for SAN Client” on page 27.

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 27.

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.	<p>Cohesity 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.</p> <p>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.</p>
Be aware of performance degradation when a port is configured for multiple zones.	<p>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.</p>

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

Guideline	Description
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.
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 35.

Table 3-3 Fibre Channel zones

Zone	Description
A Fibre Transport zone	<p>A Fibre Transport zone (or backup zone) should include only specific HBA ports of the hosts that use Fibre Transport, as follows:</p> <ul style="list-style-type: none"> ■ Ports on the FT media server HBAs that connect to the SAN clients. These ports use the Cohesity target mode driver. See “About the target mode driver” on page 33. ■ 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.

Table 3-3 Fibre Channel zones (*continued*)

Zone	Description
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 zoning the SAN for Fibre Transport for a 16-gigabit target mode HBA support

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 27.

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 3-4](#) describes the best practices for zoning the SAN on NetBackup appliances and NBU FTMS with 16Gb and 32Gb HBA.

Table 3-4 Best practices for zoning the SAN on NetBackup appliances

Guideline	Description
One initiator per zone, multiple targets acceptable.	<p>Cohesity 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.</p> <p>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.</p>

Table 3-4 Best practices for zoning the SAN on NetBackup appliances
(continued)

Guideline	Description
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.
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.

Note: To enable the SAN client 16-GB target mode driver support for HBA ports, you must create zones with only one initiator and keep only one target mode per zone.

[Table 3-5](#) 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 35.

Table 3-5 Fibre Channel zones

Zone	Description
A Fibre Transport zone	<p>A Fibre Transport zone (or backup zone) should include only specific HBA ports of the hosts that use Fibre Transport, as follows:</p> <ul style="list-style-type: none"> ■ Ports on the FT media server HBAs that connect to the SAN clients. These ports use the Cohesity target mode driver. See “About the target mode driver” on page 33. ■ 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	<p>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.</p>

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.

About the 16-gigabit target mode HBAs for SAN clients and Fibre Transport media servers

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 or Emulex 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 34.
- 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.

Note: To enable the SAN client 16-GB target mode driver support for HBA ports, you must create zones with only one initiator and keep only one target mode per zone. Each NetBackup client can have a zone with only one Fibre Transport media server.

For information about supported HBAs, see the [Hardware Compatibility List](#).

See [“Preparing the SAN”](#) on page 20.

About the 16-gigabit target mode 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.

HBA 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 or an Emulex HBA that NetBackup supports for Fibre Transport. For these HBAs, you must configure them to use the NetBackup target mode driver.
- QLogic HBA and Emulex HBA cannot be used as target mode at the same time. You must choose one of them as target mode.
- When QLogic HBA is used as target, you can use Emulex HBA to work as initiators if initiator HBA is needed.

For information about supported HBAs, see the hardware compatibility list at the following URL:

<http://www.netbackup.com/compatibility>

See “Preparing the SAN” on page 20.

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.

Licensing SAN Client and Fibre Transport

This chapter includes the following topics:

- [About SAN Client installation](#)
- [About the SAN Client license](#)
- [When upgrading SAN Client and Fibre Transport](#)

About SAN Client installation

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

See [“About the SAN Client license”](#) on page 29.

About the SAN Client license

On the NetBackup primary server, enter the license that activates the SAN Client feature.

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.veritas.com/docs/DOC5332>

Configuring SAN Client and Fibre Transport

This chapter includes the following topics:

- [Overview of configuring SAN Client and Fibre Transport](#)
- [Configuring a Fibre Transport media server](#)
- [Configuring SAN clients](#)
- [Configuring SAN clients in a cluster](#)
- [About configuring Fibre Transport properties](#)
- [Configure Fibre Transport properties](#)
- [Fibre Transport properties](#)
- [Configure SAN client usage preferences](#)
- [SAN client usage preferences](#)

Overview of configuring SAN Client and Fibre Transport

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

All of the NetBackup hosts that you use for SAN Client and Fibre Transport must be provisioned with host ID-based security certificates. The hosts must be able to communicate with each other.

[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 32.
Step 2	Configure the SAN clients	See “Configuring SAN clients” on page 52. See “Configuring SAN clients in a cluster” on page 55.
Step 3	Configure FT properties	See “About configuring Fibre Transport properties” on page 58.
Step 4	Configure SAN client usage preferences	See “SAN client usage preferences” on page 64.

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 63. See “About HBAs for SAN clients and Fibre Transport media servers” on page 25. See “About the target mode driver” on page 33. See “About nbhba mode and the ql2300_stub driver” on page 34. See “About FC attached devices” on page 34. See “How to identify the HBA ports” on page 35. See “About HBA port detection on Solaris” on page 36. See “About Fibre Transport media servers and VLANs” on page 36.
Step 2	Start nbhba mode on the media server	See “Start nbhba mode” on page 37.
Step 3	Mark the HBA ports	See “Mark the Fibre Transport media server HBA ports” on page 38.
Step 4	Configure the FT services	See “Configure the media server Fibre Transport services” on page 41.

Configuring a Fibre Transport media server with a 16-gigabit target mode HBA support

Table 5-3 Process to configure an FT media server with a 16-gigabit target mode HBA support

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 63. See “About the target mode driver” on page 33. See “About Fibre Transport media servers and VLANs” on page 36.
Step 2	Configure the FT services	See “Configure the media server Fibre Transport services for a 16-gigabit target mode HBA support” on page 45.
Step 3	Displaying the FTMS state for a 16-gigabit target mode HBA support (Optional)	See “Display the FTMS state for a 16-gigabit target mode HBA support” on page 51.
Step 4	Identifying the HBA ports for a 16-gigabit target mode HBA support (Optional)	See “Identify the HBA ports for a 16-gigabit target mode HBA support” on page 51.

About the target mode driver

On NetBackup FT media servers, QLogic or Emulex Fibre Channel host bus adapter (HBA) ports connect to the NetBackup SAN clients. Cohesity 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 or Emulex HBAs; the target mode configuration process affects only QLogic or Emulex 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 63.

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 Cohesity provided `ql2300_stub` driver to all QLogic ISP2312 and ISP24xx 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 Cohesity modules load”](#) on page 84.

About FC attached devices

In `nbhba` mode, all devices that are attached to QLogic ISP2312 and ISP24xx 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 ISP24xx 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 [“Disable a Fibre Transport media server”](#) on page 72.

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/opensv/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, target ports on more than one bus are supported on Solaris 10.

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 in the **Additional servers** list. This list appears in the 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 primary 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 `ipconfig -all` command to display host and domain information.

See [“Backups failover to LAN even though Fibre Transport devices available”](#) on page 83.

Start 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/opensv/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 Cohesity modules load”](#) on page 84.

- 4 Continue by marking the HBA ports.

See [“Mark the Fibre Transport media server HBA ports”](#) on page 38.

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/opensv/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 Restart the host.
- 5 Continue by marking the HBA ports.

See [“Mark the Fibre Transport media server HBA ports”](#) on page 38.

Mark 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 [“Start `nbhba` mode”](#) on page 37.

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/opensv/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/opensv/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/opensv/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/opensv/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 “[Configure the media server Fibre Transport services](#)” on page 41.

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

Configure 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 (`nbftsrv` 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 startup 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 already bound 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.

Note: After you configure the Fibre Transport media servers using the `nbftsrv_config` and the `nbftserver` scripts, reload the target driver for the HBA port on the NetBackup SAN clients that were used for backup and restore. This step ensures that the client operating system detects the tape devices that the Fibre Transport media servers export. Alternatively, you can restart the client computers to reload the drivers and refresh the device tree.

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/opensv/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 restart 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 restart when prompted. The stub driver binds to the marked ports during the start 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 restart, 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, restart 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/opensv/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 Restart the host.

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

Configure the media server Fibre Transport services for a 16-gigabit target mode HBA support

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). One service (`nbftsrvr`) comprises of 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 startup scripts.
- Starts the FT server.

When the FT server starts, the NetBackup target mode driver binds automatically to the QLogic or Emulex HBA ports. The HBA ports operate in target mode until you disable FTMS.

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](#)

You must be the root user.

Note: Additional steps are required after you configure the Fibre Transport media servers using the `nbftsrv_config` and the `nbftserver` scripts: reload the target driver for the HBA port on the NetBackup SAN clients that were used for backup and restore. This step ensures that the client operating system detects the tape devices that the Fibre Transport media servers export. Alternatively, you can restart the client computers to reload the drivers and refresh the device tree.

If you plan to use Emulex LPe31000/LPe35000 Series as the target mode HBAs, ensure that the firmware versions are supported. If the firmware is not supported, upgrade it to the specific version before configuring SAN Client and Fibre Transport. For information about the supported firmware versions, see the hardware compatibility list at the following location:

<http://www.netbackup.com/compatibility>

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/opensv/netbackup/bin/admincmd/nbftsrv_config -scst -install
Checking for SCST drivers and firmwares in the package. [yes]
Checking if the server is not NetBackup Appliance. [yes]
Checking for kernel version 4.18.0-372.9.1. [yes]
Checking for QLogic QLE2562 8Gb or QLE2692 16Gb or QLE2770
QLE2772 32Gb, or other supported QLogic 16/32Gb HBA cards on
the server. [yes]
Checking for Emulex LPe31002 16Gb, LPe31004 16Gb, and other
supported Emulex 32Gb HBA cards on the server. [yes]
```

DISCLAIMER:

NOTE:

1. When you install the SAN client with 16Gb/32Gb HBA, the script stops the original `qla2xxx` and `lpfc` driver and updates the firmware `ql2500_fw.bin`. QLogic QLE2562 8Gb and QLE2692 16Gb and QLE2770 QLE2772 32Gb HBA models, Emulex LPe31002 16Gb, LPe31004 16Gb, and other qualified QLogic/Emulex 32Gb HBA models are supported by this NetBackup version.
2. Ensure that there is no other process that uses the HBAs. If there is an active process that uses `qla2xxx` or `lpfc`, manually restart the process after the installation completes.
3. If you use the SANSurfer agent during the deployment of the environment, the script stops and restarts the SANSurfer agent daemon (`qlremote`).
4. Stop all the backup jobs that use the FT user interface.

Do you acknowledge this disclaimer? [y,n] (n) y

2 The QLogic drivers are reloaded so that the HBA ports can be detected during this session.

Proceeding to deploy SCST environment [ok]

Stopping the NetBackup Fibre Transport Server.

Waiting for nbftsrvr to shut down (this may take some time).

HBA-Type Speed	Port WWN	Status	Supported Speeds	Current
LPe31000-M6-D	10:00:00:10:9b:df:92:0e	Online	4 Gbit, 8 Gbit, 16 Gbit	16 Gbit
QLE2772	21:00:f4:c7:aa:0c:2a:87	Online	8 Gbit, 16 Gbit, 32 Gbit	32 Gbit
QLE2692	21:00:f4:c7:aa:0b:d6:88	Online	4 Gbit, 8 Gbit, 16 Gbit	16 Gbit
QLE2692	21:00:f4:c7:aa:0b:d6:89	Online	4 Gbit, 8 Gbit, 16 Gbit	16 Gbit
QLE2772	21:00:f4:c7:aa:0c:2a:86	Online	8 Gbit, 16 Gbit, 32 Gbit	32 Gbit
LPe35000-M2-D	10:00:00:10:9b:f1:63:a8	Linkdown	8 Gbit, 16 Gbit, 32 Gbit	unknown

NOTE:

The types of HBA cards listed below are filtered by the chip model. All of these HBA cards are not verified. Choose supported HBA card according to NetBackup hardware compatibility list. Some of the WWNs may be used to connect to an external storage and other external devices.

Do you want to continue? [y,n] (n)

3 Enter the port numbers and make sure of the operation warnings during this session.

```
Please input the Port WWNs you want to use as the targets (separated by commas like:
wwn1,wwn2...):10:00:00:10:9b:1d:4c:6a,10:00:00:10:9b:1d:4c:6b
The input is: 10:00:00:10:9b:1d:4c:6a,10:00:00:10:9b:1d:4c:6b
The targets you defined are Emulex HBAs
The targets you defined: 10:00:00:10:9b:1d:4c:6a 10:00:00:10:9b:1d:4c:6b
Do you want to redefine the targets? [y,n] (n) n
Do you want to add additional targets? [y,n] (n) n
The targets you defined: 10:00:00:10:9b:1d:4c:6a 10:00:00:10:9b:1d:4c:6b
The targets you have defined contain 16Gb HBA cards.
```

NOTE:

1. Make sure that you do not use a WWN that is used to connect to external storage.
 2. Make sure to define the input WWNs as targets.
 3. Make sure the WWNs can be zoned with WWNs of clients.
- Do you want to continue to setup the WWNs as targets? [y,n] (n) y

4 The FTMS environment is deployed.

```
-----  

FTMS environment installation started.  

-----
```

```
Successfully created the dependent path: /var/lib/scst/pr.  

Successfully created the dependent path: /var/lib/scst/vdev_mode_pages.  

Successfully copied /usr/opensv/netbackup/bin/driver/lancerg6_A12.8.340.8.grp to  

/lib/firmware/LPE31004.grp.  

Successfully copied  

/usr/opensv/netbackup/bin/driver/scst/ocs_fc_scst.ko.3.10.0-1160.el7.x86_64 to  

/lib/modules/3.10.0-1160.15.2.el7.x86_64/extra/ocs_fc_scst.ko.  

Successfully copied /usr/opensv/netbackup/bin/driver/scst/scst.ko.3.10.0-1160.el7.x86_64  

to /lib/modules/3.10.0-1160.15.2.el7.x86_64/extra/scst.ko.  

Successfully copied  

/usr/opensv/netbackup/bin/driver/scst/scst_user.ko.3.10.0-1160.el7.x86_64 to  

/lib/modules/3.10.0-1160.15.2.el7.x86_64/extra/scst_user.ko.  

Successfully created /etc/modprobe.d/ocs_fc_scst.conf.  

Successfully copied /usr/opensv/netbackup/bin/nbftsrvr to  

/usr/opensv/netbackup/bin/nbftsrvr_old.  

Successfully copied /usr/opensv/netbackup/bin/goodies/nbftserver_scst to  

/etc/rc.d/init.d/nbftserver.  

Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc2.d/S21nbftserver.  

Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc3.d/S21nbftserver.  

Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc5.d/S21nbftserver.  

Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc0.d/K03nbftserver.  

Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc1.d/K03nbftserver.  

Successfully linked /etc/rc.d/init.d/nbftserver /etc/rc.d/rc6.d/K03nbftserver.  

Successfully enabled nbftserver.  

Successfully created /etc/modules-load.d/scst.conf.  

Successfully find PCIID:0000:07:00.0 for target:10:00:00:10:9b:1d:4c:6a  

Successfully find PCIID:0000:07:00.1 for target:10:00:00:10:9b:1d:4c:6b  

Successfully bind target mode for pciid: 0000:07:00.0.  

Successfully bind target mode for pciid: 0000:07:00.1.  

Successfully rebind emulex target ports.  

Successfully modify the attribute of  

/sys/kernel/scst_tgt/targets/ocs_xe201/10:00:00:10:9b:1d:4c:6a/enabled with value 1.  

Successfully write /sys/class/fc_host/host13/issue_lip with value 1  

Enable target: 10:00:00:10:9b:1d:4c:6a  

Successfully modify the attribute of  

/sys/kernel/scst_tgt/targets/ocs_xe201/10:00:00:10:9b:1d:4c:6b/enabled with value 1.  

Successfully write /sys/class/fc_host/host14/issue_lip with value 1  

Enable target: 10:00:00:10:9b:1d:4c:6b
```

```

Previous initramfs image is saved at
/boot/initramfs-3.10.0-1160.15.2.el7.x86_64.img.03-19-21.19:31:51.
Running dracut, it may take several minutes to complete...
/sbin/dracut succeeded
Successfully moved /boot/initramfs-3.10.0-1160.15.2.el7.x86_64.img.tmp to
/boot/initramfs-3.10.0-1160.15.2.el7.x86_64.img
NetBackup Fibre Transport Server started.
-----
Driver ocs_fc_scst is loaded
-----
Driver scst is loaded
-----
Driver scst_user is loaded

-----
FTMS environment installation completed.
-----

```

Display the FTMS state for a 16-gigabit target mode HBA support

The NetBackup `nbftsrv_config` command's `-scst -state` option informs you about the state of the FTMS. The computer must have enabled FTMS for a 16/32Gb target mode HBA support.

For example:

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -scst -list_port
```

```
FTMS Target Ports List:
21:00:f4:e9:d4:53:bb:c4
```

```
FTMS daemon(nbftsrvr) state:
FTMS daemon (nbftsrvr) is running.
```

The command displays the defined FTMS target ports and the state of the FTMS daemon.

Identify the HBA ports for a 16-gigabit target mode HBA support

The NetBackup `nbftsrv_config` command's `-scst -list_port` option helps you identify the port World Wide Names (WWNs) or World Wide Port Names (WWPNs) that are defined as targets. The computer must have enabled FTMS for a 16/32 GB target mode HBA support.

For example:

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -scst -list_port
```

HBA-Type	Port WWN	Status	Current Mode	Set Mode	Supported Speeds	Current Speed
QLE2692	21:00: f4:e9:d4: 53:bb:c4	Online	Target	Target	8 Gbit, 16 Gbit	16 Gbit

Note: The types of HBA cards that get listed are QLE2772, QLE2770, QLE2692, and QLE2562 of QLogic HBA, and Emulex LPe31000/35000 Series HBA. If the QLogic HBA is used as a target, you can use Emulex HBA to work as an initiator, if an initiator HBA is required.

Configuring SAN clients

[Table 5-4](#) shows the steps to configure SAN clients.

Table 5-4 SAN Client and Fibre Transport configuration process

Step	Task	Section
Step 1	Configure firewalls on SAN clients	See “About configuring firewalls for SAN clients” on page 52.
Step 2	Configure SAN client drivers	See “SAN client driver requirements” on page 52.
Step 3	Configure the SAN client FT service	See “Configure the SAN Client Fibre Transport service” on page 53.

About configuring firewalls for SAN clients

NetBackup SAN clients require connectivity to the NetBackup primary server.

Therefore, you must ensure that any firewall (software or hardware) allows the clients to communicate with the NetBackup primary server.

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 5-5](#) lists the driver requirements for each supported SAN client operating system.

Table 5-5 SAN client operating system driver requirements

Operating system	Driver requirements
AIX	<p>Client systems require the standard tape driver. The driver should work without modification.</p> <p>For information about how to configure the driver, see the <i>NetBackup Device Configuration Guide</i>, available at the following URL:</p> <p>http://www.veritas.com/docs/DOC5332</p>
Linux	<p>Client systems require the SCSI Generic (<code>sg</code>) driver and pass-through device files.</p> <p>For information about how to configure the driver, see the <i>NetBackup Device Configuration Guide</i>, available at the following URL:</p> <p>http://www.veritas.com/docs/DOC5332</p>
Solaris	<p>You must modify the <code>/kernel/drv/st.conf</code> file so that Solaris recognizes the FT devices on the NetBackup media servers.</p> <p>For information about how to do so, see the <i>NetBackup Device Configuration Guide</i>, available at the following URL:</p> <p>http://www.veritas.com/docs/DOC5332</p>
Windows	<p>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.</p>

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

<http://www.veritas.com/docs/DOC5332>

Configure 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 55.

See [“Register a SAN client cluster virtual name”](#) on page 56.

To configure a NetBackup client to be a SAN client

- 1 Verify that the PBX service is active on the client, as follows:
 - On UNIX and Linux systems, run the `NetBackup bpps -x` command and verify that the `pbx_exchange` process is active.
 - On Windows systems, use the Computer Management console to verify that the 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/opensv/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: Start 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 and Solaris: Run the NetBackup `bp.start_all` command. The command resides in the following directory:
`/usr/opensv/netbackup/bin`
 - Windows: Start the system, which also begins operating system device discovery.

- 4 On the systems that were not started 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 84.

After the client OS discovers the FT devices, the SAN client is registered with NetBackup.

- 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 [“Rescan for Fibre Transport devices from a SAN client”](#) on page 67.

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 57.

See [“Configuring SAN clients”](#) on page 52.

Table 5-6 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 .

Table 5-6 Process to configure a SAN client in a cluster (*continued*)

Step	Action	Description
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 for SAN clients” on page 52. See “SAN client driver requirements” on page 52. See “Configure the SAN Client Fibre Transport service” on page 53.
Step 3	Register the virtual node name with the server	See “Register a SAN client cluster virtual name” on page 56.
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 16. See “Setting NetBackup configuration options by using the command line” on page 57. Warning: Do not change the LOCAL_CACHE value on the FT media servers or the primary server.

Register a SAN client cluster virtual name

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

See [“Configuring SAN clients in a cluster”](#) on page 55.

To register a cluster virtual name

- 1 Add the virtual name to the 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/opensv/netbackup/bin/admincmd`

- **Windows:** `install_path\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

Cohesity recommends to use the NetBackup web UI to configure the host properties.

However, some properties cannot be set by using the **NetBackup web UI**. You can set those properties by using the following NetBackup commands:

For a NetBackup server: `bpsetconfig`

For a NetBackup client: `nbsetconfig`

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.example.com`

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

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 the appropriate command. The command depends on the operating system and the NetBackup host type (client or server), as follows:

UNIX On a NetBackup client:

```
/usr/opensv/netbackup/bin/nbsetconfig
```

On a NetBackup server:

```
/usr/opensv/netbackup/bin/admincmd/bpsetconfig
```

Windows On a NetBackup client:

```
install_path\NetBackup\bin\nbsetconfig.exe
```

On a 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**.

Table 5-7 Fibre Transport properties

Granularity	Description
Global Fibre Transport properties for all SAN clients	Global Fibre Transport properties apply to all SAN clients. Global Fibre Transport properties are configured on the primary server. Configure these properties in the Fibre Transport host properties for the primary server.
Fibre Transport properties for a media server or media servers	Fibre Transport 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 Fibre Transport properties that are configured on the primary server. Configure these properties in the Fibre Transport host properties for the media server.
Fibre Transport properties for a SAN client or SAN clients	Fibre Transport properties for a client or clients apply to the specific SAN client or clients. Fibre Transport properties for SAN clients override the media server FT properties. Configure these properties in the Fibre Transport host properties for the client.

See [“Configure Fibre Transport properties”](#) on page 59.

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

See [“SAN client usage preferences”](#) on page 64.

See [“Overview of configuring SAN Client and Fibre Transport”](#) on page 31.

Configure 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 58.

To configure NetBackup Fibre Transport properties

- 1 On the left, select **Hosts > Host properties**.
- 2 Depending on which level of properties you want to configure, do one of the following:

To configure global Fibre Transport properties Select the primary server. If necessary select **Connect**, then select **Edit primary server**.

To configure Fibre Transport properties for a media server or servers Select the media server. If necessary select **Connect**, then select **Edit media server**. The Fibre Transport host properties are only available for a media server if Fibre Transport services are enabled for that server.

To configure Fibre Transport properties for a client or clients Select the client. If necessary select **Connect**, then select **Edit client**.

- 3 Select **Fibre Transport**.
- 4 Configure the properties.
 See [“Fibre Transport properties”](#) on page 60.

Fibre Transport properties

To access this setting, in the web UI select **Hosts > Host properties**. Select the host. If necessary, click **Connect**. Then click **Edit primary server**, or **Edit media server**, or **Edit client**. Click **Fibre Transport**.

Note that any usage preferences that you configure for an individual SAN Client in **Storage > SAN Clients** override the Fibre Transport properties that you configure in **Host properties**.

See [“Configure SAN client usage preferences”](#) on page 64.

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, as follows:

Table 5-8 Host types for Fibre Transport properties

Host type	Description
Primary server	Global Fibre Transport properties that apply to all SAN clients.

Table 5-8 Host types for Fibre Transport properties (*continued*)

Host type	Description
Media server	The Fibre Transport Maximum concurrent Fibre Transport connections property applies to the Fibre Transport media server that you select.
Client	The Fibre Transport properties apply to the SAN client that you select. The default values for clients are the global property settings of the primary server. Client properties override the global Fibre Transport properties.

The **Fibre Transport** properties contain the following settings. All properties are not available for all hosts. In this table, the Fibre Transport 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 Fibre Transport device.

Table 5-9 Fibre Transport properties

Property	Description
Maximum concurrent Fibre Transport connections	<p>This property displays only when you select a Fibre Transport media server .</p> <p>This property specifies the number of Fibre Transport connections to allow to the selected media server or media servers. A connection is equivalent to a job.</p> <p>If no value is set, NetBackup uses the following defaults:</p> <ul style="list-style-type: none"> ■ 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. A fast port is 8 GB or faster, and a slow port is less than 8 GB. <p>You can enter up to the following maximum connections for the media server or servers to use:</p> <ul style="list-style-type: none"> ■ On a Linux Fibre Transport media server host: 40. The recommended setting is 32 or fewer connections concurrently on Linux. On Linux hosts, you can increase that maximum by setting a NetBackup touch file, <code>NUMBER_DATA_BUFFERS_FT</code>. See “About Linux concurrent FT connections” on page 63. ■ For NetBackup Appliance model 5330 and later: 40. ■ For NetBackup Appliance model 5230 and later: 40. ■ On a Solaris Fibre Transport media server host: 64. <p>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. If you have buffers per connection you see better performance for each connection.</p>
Use defaults from the primary server configuration	<p>This property displays only when you select a client .</p> <p>This property specifies that the client follow the properties as they are configured on the primary server.</p>
Preferred	<p>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.</p> <p>For the global property that is specified on the primary server, the default is Preferred.</p>

Table 5-9 Fibre Transport properties (*continued*)

Property	Description
Always	<p>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.</p> <p>However, an FT device must be active 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.</p>
Fail	<p>The Fail property specifies that NetBackup should fail the job if an FT device is not active and up. If the FT devices are active 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 are active, none have been configured, or the SAN Client license expired.</p>
Never	<p>The Never property specifies that NetBackup should never use a Fibre Transport pipe for backups and restores of SAN clients. NetBackup uses a LAN connection for the backups and restores.</p> <p>If you specify Never for the primary server, Fibre Transport is disabled in the NetBackup environment. If you select Never, you can configure Fibre Transport usage on a per-client basis.</p> <p>If you specify Never for a SAN client, Fibre Transport is disabled for the client.</p>

About Linux concurrent FT connections

NetBackup uses the **Maximum concurrent FT connections** setting in the **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 60.

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 from [Table 5-10](#) in the file:

```
/usr/opensv/netbackup/db/config/NUMBER_DATA_BUFFERS_FT
```

[Table 5-10](#) shows the values that NetBackup supports for the `NUMBER_DATA_BUFFERS_FT` file. NetBackup supports 644 buffers per media server for Fibre transport.

Table 5-10 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 with the **Maximum concurrent FT connections** setting in the **Fibre transport** host properties.

Configure SAN client usage preferences

SAN client usage preferences let you configure how a specific client uses NetBackup Fibre Transport for backups. These preferences override the Fibre Transport settings in the host properties.

See [“Fibre Transport properties”](#) on page 60.

See [“About configuring Fibre Transport properties”](#) on page 58.

To configure SAN client usage preferences

- 1 Open the NetBackup web UI and sign into the primary server.
- 2 On the left, select **Storage > SAN clients**.
- 3 Locate the SAN client.
- 4 Select **Actions > Usage preferences**.
- 5 Configure the properties.
See [“SAN client usage preferences”](#) on page 64.
- 6 Select **Save**.

SAN client usage preferences

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

Table 5-11 SAN client Fibre Transport usage preferences

Property	Description
Use defaults from the primary server configuration	This property specifies that the client follow the properties as they are configured on the primary server.
Preferred	<p>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.</p> <p>For the global property that is specified on the primary server, the default is Preferred.</p>
Always	<p>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.</p> <p>However, an FT device must be active 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.</p>
Fail	The Fail property specifies that NetBackup should fail the job if an FT device is not active and up. If the FT devices are active 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	<p>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.</p> <p>If you specify Never for a SAN client, Fibre Transport is disabled for the client.</p>

Managing SAN clients and Fibre Transport

This chapter includes the following topics:

- [Enable or disable the Fibre Transport services](#)
- [Enable or disable the Fibre Transport services for a 16-gigabit target mode HBA support](#)
- [Rescan for Fibre Transport devices from a SAN client](#)
- [View the SAN client Fibre Transport job details](#)
- [View the Fibre Transport traffic](#)
- [Delete a SAN client](#)

Enable or disable 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 service, the other service stops. If one service ends abnormally, the other service stops.

These services do not appear in the 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 Open the NetBackup web UI and sign into the primary server.
- 2 On the left, select **Storage > Media servers**.
- 3 Select the **Media servers** tab.
- 4 Select an FT media server.
- 5 Select either **Enable FT services** or **Disable FT services**.

Enable or disable the Fibre Transport services for a 16-gigabit target mode HBA support

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

The following is the service that composes the FT server:

- The `nbftsrvr` service manages the server side of the FT pipe.

This service does not appear in the Activity monitor; it does appear in the operating system process displays.

To enable or disable FT services

- 1 Open the NetBackup web UI and sign into the primary server.
- 2 On the left, select **Storage > Media servers**.
- 3 Select an FT media server.
- 4 Select either **Enable FT services** or **Disable FT services**.

Rescan 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 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 Open the NetBackup web UI and sign into the primary server.
- 2 On the left, select **Storage > SAN clients**.
- 3 Select a client.
- 4 Select **Actions > Rescan FT devices**.
- 5 Monitor the following status of the operation:
 - Initiated
 - Client system must be restarted
 - Failure
- 6 If required, restart the client system.

View the SAN client Fibre Transport job details

The Activity monitor **Jobs** tab displays all of the jobs that are in progress or have been completed.

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

The job's **Details** tab shows more detailed information about the job, including the following:

- A **Transport type** field in the header area shows the same information as in the **Jobs** tab.
- Messages in the job details show the status of jobs that use FT transport, as follows:

See [“View the Fibre Transport traffic”](#) on page 69.

To view job details

- 1 Go to the Activity monitor.
- 2 In the **Jobs** tab, select the job.

The job details contain information on the **Overview** tab and the **Details** tab.

View the 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 | <p>The media server view shows all of the inbound backup (and outbound restore) traffic for a selected FT media server.</p> <p>Use this view to determine which SAN clients can send data to and receive data from the selected media server.</p> <p>See “To view FT activity from the media server perspective” on page 69.</p> |
| SAN client view | <p>The SAN client view shows all of the outbound backup (and inbound restore) traffic for a selected client.</p> <p>Use this view to determine which FT media servers can send data to and receive data from the selected client.</p> <p>See “To view FT activity from the client perspective” on page 69.</p> |

See [“View the SAN client Fibre Transport job details”](#) on page 68.

To view FT activity from the media server perspective

- 1 Open the NetBackup web UI and sign into the primary server.
 - 2 On the left, select **Storage > Media servers**.
 - 3 Select the **Media servers** tab.
 - 4 Locate the FT media server.
 - 5 Select **Actions > View FT connections**.
- NetBackup shows the connection activity for the media server.

To view FT activity from the client perspective

- 1 Open the NetBackup web UI and sign into the primary server.
 - 2 On the left, select **Storage > SAN clients**.
 - 3 Locate the client.
 - 4 Select **Actions > View FT connections**.
- NetBackup shows the connection activity for the client.

Delete 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 Stop the client services.
- 2 Open the NetBackup web UI and sign into the primary server.
- 3 On the left, select **Storage > SAN clients**.
- 4 Locate the client.
- 5 Select **Actions > Delete**.

Disabling SAN Client and Fibre Transport

This chapter includes the following topics:

- [Disable a SAN client](#)
- [Disable a Fibre Transport media server](#)
- [Disable a Fibre Transport media server for a 16-gigabit target mode HBA support](#)

Disable a SAN client

You cannot uninstall the SAN Client and Fibre Transport components. However, you can disable the SAN clients. If you do, the client cannot backup over the SAN to an FT media server.

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

See [“Delete a SAN client”](#) on page 70.

To disable the NetBackup SAN client service on UNIX

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

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

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

```
/usr/opensv/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
```

Disable a Fibre Transport media server

You cannot uninstall the Fibre Transport components. However, you can disable the 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.

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 start. 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/opensv/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/opensv/netbackup/bin/admincmd/nbftconfig -ds  
ft_server_host_name
```

Disable a Fibre Transport media server for a 16-gigabit target mode HBA support

You cannot uninstall the Fibre Transport components. However, you can disable the FT media server and remove the operating system FT startup scripts from the media server. The process also removes the SCST and QLogic or Emulex drivers. The media server then does not support NetBackup Fibre Transport.

To disable an FT media server and remove drivers

- 1** On the FT media server, run the following script:

```
/usr/opensv/netbackup/bin/admincmd/nbftsrv_config -scst -uninstall
```

- 2** Verify that the following startup scripts were removed:

```
scripts: (/etc/rc.d/)
    /etc/rc.d/init.d/nbftserver
    /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
drivers: (lib/modules/xxx/extra)
    qla2x00tgt.ko
    qla2xxx.ko
    scst.ko
    scst_user.ko
firmwares: (/lib/firmware)
    ql2700-firmware-8.07.10.bin and ql2700_fw.bin
    ql2500-firmware-8.04.00.bin and ql2500_fw.bin
folders:
    /var/lib/scst/vdev_mode_pages
    /var/lib/scst/pr
    /usr/share/doc/ql2500-firmware-8.04.00
/etc/modules-load.d/scst.conf
```

- 3** If the startup scripts were not removed, delete them manually. After you remove the files, rename `ql2500_fw_original.bin` to `ql2500_fw.bin`.

- 4** Run the following script:

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

Note: If your `/boot` partition does not have enough disk space, manually delete images like

`initramfs-3.10.0-514.26.2.el7.x86_64.img.10-23-17.17:22:37` to get more disk space.

Troubleshooting SAN Client and Fibre Transport

This chapter includes the following topics:

- [About troubleshooting SAN Client and Fibre Transport](#)
- [SAN Client troubleshooting tech note](#)
- [View the Fibre Transport logs](#)
- [About unified logging](#)
- [Stop and start the Fibre Transport services](#)
- [Stop and start the Fibre Transport services for a 16-gigabit target mode HBA support](#)
- [Backups failover to LAN even though Fibre Transport devices available](#)
- [Kernel warning messages when Cohesity modules load](#)
- [SAN client service does not start](#)
- [SAN Client Fibre Transport Service validation](#)
- [SAN client does not select Fibre Transport](#)
- [Media server Fibre Transport device is not active](#)
- [No Fibre Transport devices discovered](#)

About troubleshooting SAN Client and Fibre Transport

SAN Client and Fibre Transport troubleshooting information is available.

See [“SAN Client troubleshooting tech note”](#) on page 76.

See [“View the Fibre Transport logs”](#) on page 76.

See [“Stop and start the Fibre Transport services”](#) on page 81.

See [“Backups failover to LAN even though Fibre Transport devices available ”](#) on page 83.

See [“SAN client service does not start”](#) on page 84.

See [“SAN Client Fibre Transport Service validation”](#) on page 84.

See [“SAN client does not select Fibre Transport”](#) on page 85.

See [“Media server Fibre Transport device is not active”](#) on page 86.

See [“No Fibre Transport devices discovered”](#) on page 87.

SAN Client troubleshooting tech note

More troubleshooting information about SAN clients and Fibre Transport is available on the Cohesity Technical Support website in the following Tech Note:

https://www.veritas.com/content/support/en_US/article.100029180

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

View the Fibre Transport logs

You can monitor Fibre Transport activity and status by viewing the log messages that the FT processes generate. Unified Logging (VxUL) uses 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	<p><code>nbftsrvr</code> and <code>nbfdrv64</code>. The media server Fibre Transport services.</p> <p>For a 16-gigabit target mode HBA support only <code>nbftsrvr</code> is supported. The media server Fibre Transport services.</p> <p>Note: You can use only one of the two methods.</p>
200	<code>nbftclnt</code> . 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 77.

Configure the amount of information that is collected and its retention length on the NetBackup primary server in the **Logging** properties and **Clean-up** properties. Information about these properties is available in the [NetBackup Web UI Administrator’s Guide](#).

See [“About troubleshooting SAN Client and Fibre Transport”](#) on page 76.

About unified logging

Unified logging creates log file names and messages in a format that is standardized across Cohesity products. Only the `vxlogview` command can assemble and display the log information correctly. Server processes and client processes use unified logging.

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/opensv/logs`

Note: Only the following types of users can access the logs: root and service users in Linux systems, and users present in the administrators group of Windows systems.

You can access logging controls in **Logging** host properties. You can also manage unified logging with 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 80.

About using the `vxlogview` command to view unified logs

Only the `vxlogview` command can assemble and display the unified logging information correctly. The unified logging files are in binary format and some of the information is contained in an associated resource file. These logs are stored in the following directory. You can display `vxlogview` results faster by restricting the search to the files of a specific process.

- UNIX `/usr/openv/logs`
- Windows `install_path\NetBackup\logs`

Table 8-2 Fields in `vxlogview` query strings

Field name	Type	Description	Example
PRODID	Integer or string	Provide the product ID or the abbreviated name of product.	PRODID = 51216 PRODID = 'NBU'
ORGID	Integer or string	Provide the originator ID or the abbreviated name of the component.	ORGID = 116 ORGID = 'nbpem'
PID	Long Integer	Provide the process ID	PID = 1234567
TID	Long Integer	Provide the thread ID	TID = 2874950
STDATE	Long Integer or string	Provide the start date in seconds or in the locale-specific short date and time format. For example, a locale can have the format 'mm/dd/yy hh:mm:ss AM/PM'	STDATE = 98736352 STDATE = '4/26/11 11:01:00 AM'

Table 8-2 Fields in vxlogview query strings (*continued*)

Field name	Type	Description	Example
ENDATE	Long Integer or string	Provide the end date in seconds or in the locale-specific short date and time format. For example, a locale can have the format 'mm/dd/yy hh:mm:ss AM/PM'	ENDATE = 99736352 ENDATE = '04/27/11 10:01:00 AM'
PREVTIME	String	Provide the hours in 'hh:mm:ss' format. This field should be used only with operators =, <, >, >=, and <=	PREVTIME = '2:34:00'
SEV	Integer	Provide one of the following possible severity types: 0 = INFO 1 = WARNING 2 = ERR 3 = CRIT 4 = EMERG	SEV = 0 SEV = INFO
MSGTYPE	Integer	Provide one of the following possible message types: 0 = DEBUG (debug messages) 1 = DIAG (diagnostic messages) 2 = APP (application messages) 3 = CTX (context messages) 4 = AUDIT (audit messages)	MSGTYPE = 1 MSGTYPE = DIAG
CTX	Integer or string	Provide the context token as string identifier or 'ALL' to get all the context instances to be displayed. This field should be used only with the operators = and !=.	CTX = 78 CTX = 'ALL'

Table 8-3 Examples of query strings with dates

Example	Description
<code>((PRODID == 51216) && ((PID == 178964) ((STDATE == '2/5/15 09:00:00 AM') && (ENDATE == '2/5/15 12:00:00 PM'))))</code>	Retrieves the log file message for the NetBackup product ID 51216 between 9AM and 12PM on 2015-05-02.
<code>((prodid = 'NBU') && ((stdate >= '11/18/14 00:00:00 AM') && (enddate <= '12/13/14 12:00:00 PM')))) ((prodid = 'BENT') && ((stdate >= '12/12/14 00:00:00 AM') && (enddate <= '12/25/14 12:00:00 PM'))))</code>	Retrieves the log messages for the NetBackup product NBU between 2014-18-11 and 2014-13-12 and the log messages for the NetBackup product BENT between 2014-12-12 and 2014-25-12.
<code>(STDATE <= '04/05/15 0:0:0 AM')</code>	Retrieves the log messages that were logged on or before 2015-05-04 for all of the installed Cohesity products.

Examples of using vxlogview to view unified logs

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

Note: Only the following types of users can access the logs: root and service users in Linux systems, and users present in the administrators group of Windows systems.

Table 8-4 Example uses of the vxlogview command

Item	Example
Display all the attributes of the log messages	<code>vxlogview -p 51216 -d all</code>
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: <code>vxlogview --prodid 51216 --display D,T,m,x</code>
Display the latest log messages	Display the log messages for originator 116 (<code>nbpem</code>) that were issued during the last 20 minutes. Note that you can specify <code>-o nbpem</code> instead of <code>-o 116</code> : <code># vxlogview -o 116 -t 00:20:00</code>

Table 8-4 Example uses of the vxlogview command (*continued*)

Item	Example
Display the log messages from a specific time period	<p>Display the log messages for <code>nbpem</code> that were issued during the specified time period:</p> <pre># vxlogview -o nbpem -b "05/03/15 06:51:48 AM" -e "05/03/15 06:52:48 AM"</pre>
Display results faster	<p>You can use the <code>-i</code> option to specify an originator for a process:</p> <pre># vxlogview -i nbpem</pre> <p>The <code>vxlogview -i</code> option searches only the log files that the specified process (<code>nbpem</code>) creates. By limiting the log files that it has to search, <code>vxlogview</code> returns a result faster. By comparison, the <code>vxlogview -o</code> option searches all unified log files for the messages that the specified process has logged.</p> <p>Note: If you use the <code>-i</code> option with a process that is not a service, <code>vxlogview</code> 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 <code>-o</code> option instead of the <code>-i</code> option.</p> <p>The <code>-i</code> option displays entries for all OIDs that are part of that process including libraries (137, 156, 309, etc.).</p>
Search for a job ID	<p>You can search the logs for a particular job ID:</p> <pre># vxlogview -i nbpem grep "jobid=job_ID"</pre> <p>The <code>jobid=</code> search key should contain no spaces and must be lowercase.</p> <p>When searching for a job ID, you can use any <code>vxlogview</code> command option. This example uses the <code>-i</code> option with the name of the process (<code>nbpem</code>). 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 <code>jobid=job_ID</code>.</p>

Stop and start the 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:

Stop and start the Fibre Transport services for a 16-gigabit target mode HBA support

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 Cohesity support engineer may direct you to stop and restart services for troubleshooting purposes.

See [“Enable or disable the Fibre Transport services”](#) on page 66.

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 `nbfdvr64` process. It does not allow the process to stop gracefully, and the SAN clients cannot detect the FT devices when the `nbfdvr64` process dies. You then may have to reboot the client systems so they detect the FT devices again (after you restart `nbfdvr64`).

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

Stop and start the Fibre Transport services for a 16-gigabit target mode HBA support

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 `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 Cohesity support engineer may direct you to stop and restart services for troubleshooting purposes.

See [“Enable or disable the Fibre Transport services”](#) on page 66.

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.

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 36.

For all of the hosts that participate in the backups, examine their **Additional servers** lists on in the **Servers** host properties. 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 8-5 How to fix an incorrect host name order in NetBackup

Task	Procedure
Stop the FT services on the media server	See “Enable or disable the Fibre Transport services” on page 66.
Delete the FT server from the NetBackup database	Use the following NetBackup command to delete the host from the NetBackup database as an FT media server: <pre>nbftconfig -deleteserver -Me <i>hostname</i></pre> The host remains in the database as a NetBackup media server.
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 Web UI Administrator’s Guide .
Start the FT services on the media server	See “Enable or disable the Fibre Transport services” on page 66.
Scan for FT devices from each SAN client	When the FT media server is discovered during the rescan operation, NetBackup adds it to the database as an FT media server. See “Rescan for Fibre Transport devices from a SAN client” on page 67.

Kernel warning messages when Cohesity modules load

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

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

The messages appear because the Cohesity 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/opensv/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 Fibre Transport device state to “not active” for all Fibre Transport target devices in the client's SAN zone. (For other clients in the zone that pass the validation, the Fibre Transport devices are active.)

To see the FT device state from the client, on the left select **Storage > SAN clients**. Locate the SAN client, then select **Actions > View FT devices**.

The check driver messages in the `nbftcInt` 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 [“View the Fibre Transport logs”](#) on page 76.

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 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:

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

Media server Fibre Transport device is not active

If NetBackup shows that a media server FT device is not active, the selected SAN client cannot detect the target mode driver on that media server. The FT device state displays in **Storage > SAN clients**. Select the SAN client and then select **Actions > View FT devices**. (An FT device represents the HBA target mode driver on a media server.)

An FT device may be “not active” 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 84.

If all media server FT devices for a client are not active, 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 [“Stop and start the Fibre Transport services”](#) on page 81.

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

See [“View the Fibre Transport logs”](#) on page 76.

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.veritas.com/docs/DOC5332>

AIX specific configuration details

This appendix includes the following topics:

- [AIX Reference Information](#)
- [Before you begin configuring NetBackup on AIX](#)
- [About AIX persistent naming support](#)
- [About configuring robotic control device files in AIX](#)
- [About device files for SAN Clients on AIX](#)
- [About non-QIC tape drives on AIX](#)
- [About no rewind device files on AIX](#)
- [Create AIX no rewind device files for tape drives](#)
- [Disable the AIX dynamic tracking](#)

AIX Reference Information

The following information is specific to AIX. Certain devices, such as tape or robotic devices, have specific AIX configuration requirements. This AIX reference section contains relevant information.

Before you begin configuring NetBackup on AIX

Observe the following points when you configure the operating system:

- Verify that NetBackup supports your server platform and devices. Download the NetBackup hardware and operating system compatibility lists.
<http://www.netbackup.com/compatibility>
- Attach all peripherals and reboot the system before you configure the devices in NetBackup. When the computer is rebooted, AIX creates the device files for the attached peripherals.
- For many configuration steps, you can use the `smit` System Management Interface Tool. For more information, see the `smit(1)` man page.
- To verify that the devices are configured correctly, use `smit` and `/usr/sbin/lsdev` command.
- To obtain error and debug information about devices and robotic software daemons, the `syslogd` daemon must be active. See the AIX `syslogd(1)` man page for more information.

After you configure the hardware, add the robots and the drives to NetBackup.

About AIX persistent naming support

NetBackup requires that you enable persistent naming support for the AIX device files. Doing so ensures that the device targets and LUNs do not change after a system restart.

To enable persistent naming support, use the AIX SMIT utility or the `chdev` command to change the logical names of the devices. Change the logical names after the initial device configuration in AIX. For more information, see the IBM documentation.

About configuring robotic control device files in AIX

NetBackup discovers the device files when you configure devices.

For information about the driver and how to configure device files, see the IBM documentation.

For robotic libraries other than IBM, Cohesity recommends that you use an operating system other than AIX as the robotic control host.

About device files for SAN Clients on AIX

NetBackup SAN clients use tape drivers and SCSI pass-through methods for Fibre Transport traffic to NetBackup FT media servers. An AIX SAN Client that uses the

standard tape driver can discover Fibre Transport targets on the FT media servers. The media server FT devices appear as `ARCHIVE Python` tape devices during SCSI inquiry from the SAN client. However, they are not tape devices and do not appear as tape devices in NetBackup device discovery.

During system startup, the AIX `cfgmgr` command configures all the devices that are necessary to use the system. If a NetBackup SAN Client cannot discover the FT devices, you can configure the device files on the client manually. Use the same procedure that you use for tape devices.

About non-QIC tape drives on AIX

Variable length block and fixed length block refer to how the operating system reads from and writes to a tape. Variable-mode devices allow more flexibility to read previously written tapes. Many tape devices can be accessed in either mode. NetBackup assumes variable length for non-quarter inch cartridge (QIC) drives.

For more information, see the `chdev(1)` and `smit(1)` man pages and the system management guide. The `smit` application is the most convenient way to change from fixed to variable-length-block devices manually.

Warning: For NetBackup, you must configure non-QIC tape drives as variable-length-block devices. Otherwise NetBackup can write data but may not be able to read it correctly. During a read, you may see a `not in tar` format error.

When you add a non-QIC tape drive to NetBackup, NetBackup issues the `chdev` command to configure the drive as a variable length block device. For reference, the following is the command that NetBackup uses to configure a drive for variable mode:

```
/usr/sbin/chdev -l Dev -a block_size=0
```

Dev represents the logical identifier for the drive (for example: `rmt0` or `rmt1`).

Therefore, you do not have to configure the drive manually for variable mode.

About no rewind device files on AIX

By default, NetBackup uses no rewind device files. These SCSI device files are in the `/dev` directory and have the following format:

```
/dev/rmtID.1
```

ID is the logical identifier assigned to the device by the system. The .1 extension specifies the no rewind, no retention on open device file.

Normally, AIX creates tape drive device files automatically at boot time. Alternatively, you can run the AIX `cfgmgr` command, which should create the device files. If they do not exist, you must create them for the tape drives.

Create AIX no rewind device files for tape drives

NetBackup uses no rewind device files for tape drives and for NetBackup SAN Clients. During system startup, the AIX `cfgmgr` command configures all the devices that are necessary to use the system. If necessary, you can use the following procedure to check for and create a no rewind device file.

To check for and create a no rewind device file

- 1 Display the I/O controllers in the system by using the following command:

```
/usr/sbin/lsdev -C | grep I/O
```

The following sample output shows that SCSI controller 1 (00-01) has been assigned the logical identifier `scsi0`.

```
scsi0 Available 00-01 SCSI I/O Controller
```

- 2 Display the SCSI and Fibre Channel devices in the system by using the following command. For SCSI devices, use `scsi` for the *type*; for Fibre Channel Protocol devices, use `fcp` for the *type*.

```
/usr/sbin/lsdev -C -s type
```

The following example shows two disk drives and a tape drive:

```
hdisk0 Available 00-01-00-0,0 400 MB SCSI Disk Drive
hdisk1 Available 00-01-00-1,0 400 MB SCSI Disk Drive
rmt0 Available 00-01-00-3,0 Other SCSI Tape Drive
```

If the device files for the tape drives exist, they appear in the output as `rmt0`, `rmt1`, and so on. The previous example output shows `rmt0`.

- 3 If a device file does not exist for the wanted tape drive, create it by using the following command:

```
/usr/sbin/mkdev -c tape -s scsi -t ost -p controller -w id,lun
```

The following are the arguments for the command:

- *controller* is the logical identifier of the drive's SCSI adapter, such as *scsi0*, *fscsi0*, or *vscsi1*.
 - *scsi_id* is the SCSI ID of the drive connection.
 - *lun* is the logical unit number of the drive connection.
- 4 To verify, display the SCSI device files by using the `lsdev` command, as follows:

```
/usr/sbin/lsdev -C -s scsi
hdisk0 Available 00-01-00-0,0 400 MB SCSI Disk Drive
hdisk1 Available 00-01-00-1,0 400 MB SCSI Disk Drive
rmt0 Available 00-01-00-3,0 Other SCSI Tape Drive
rmt1 Available 00-01-00-5,0 Other SCSI Tape Drive
```

The output shows that the `rmt1` device file was created.

- 5 If the device files do not exist on an FCP controller, use the following command to create them:

```
/usr/sbin/cfgmgr -l device
```

device is the controller number from step 1.

- 6 Ensure that the device is configured for variable-mode and extended file marks. Use the `chdev` command, as follows (*dev* is the logical identifier for the drive (for example, `rmt1`)).

```
/usr/sbin/chdev -l dev -a block_size=0
/usr/sbin/chdev -l dev -a extfm=yes
```

- 7 To configure the drive manually in NetBackup, enter the following device file pathname:

```
/dev/rmt1.1
```

Disable the AIX dynamic tracking

The AIX dynamic tracking may cause issues with the NetBackup AIX SAN Client backup jobs.

IBM AIX dynamic tracking of Fibre Channel devices is controlled by a new `fscsi` device attribute `dyntrk`.

From the AIX NetBackup SAN Client host, the AIX Fibre Channel I/O parameters for dynamic tracking and `FC_ERROR_RECOV` must be disabled. It helps to prevent the

write buffer failure to NetBackup and helps run NetBackup AIX SAN Client backup jobs without any issues.

To disable the AIX dynamic tracking

- 1 Update the `dyntrk` and `FC_ERROR_RECOV` attributes as follows to disable the AIX dynamic tracking:

- `chdev -l fscsi<fibre channel device ID> -a dyntrk=no`

For example, `chdev -l fscsi0 -a dyntrk=no`

- `chdev -l fscsi<fibre channel device ID> -a fc_err_recov=delayed_fail`

For example, `chdev -l fscsi0 -a fc_err_recov=delayed_fail`

- 2 Verify that the changes are applied.

```
lsattr -E -l fscsi<device ID>
```

For information about the IBM AIX dynamic tracking of Fibre Channel devices, see the IBM documentation.