Symantec TechNote 288437

NetBackup SAN Client and Fibre Transport Troubleshooting Guide

Revision F

1 Introduction

This document explains how to troubleshoot different failures that may occur while using the NetBackup SAN Client and Fibre Transport features. Configuring and using the SAN Client feature can require interaction with different SAN hardware devices on multiple platforms. For this reason, issues encountered using the SAN Client can often be traced back to some necessary configuration of a driver or operating system.

2 What are the components of the SAN Client feature?

In NetBackup, the SAN Client feature is comprised of three parts: SAN Clients, Fibre Transport Media Servers, and the Fibre Service Manager.

SAN Clients are actually standalone NetBackup Clients with a service enabled that allows the client to send data for backup and restores across a SAN fabric to a Media Server. The SAN Client service is available on a subset of the NetBackup Tier one clients including Solaris, Windows, Linux, HP-UX, and AIX. The VxUL logging ID for the SAN Client service is 200.

The Media Server used for these SAN transfers is referred to as a Fibre Transport Media Server because of the Fibre Transport services which are used to present Target Devices on a SAN. Only 64bit Solaris SPARC and Linux x86_64 platforms are supported as Fibre Transport servers. The Fibre Transport services include driver level components which operate on a device level with QLogic hardware. The VxUL logging ID for the Fibre Transport service is 199.

The Master Server includes a FT Service Manager (FSM) table in the EMM database. FSM is the component that tracks the status and configuration of SAN Clients and Media Servers. FSM is also used to manage the relationships of SAN Clients and Fibre Transport Media Servers to determine whether a NetBackup data transfer is eligible for a Fibre Transport. The VxUL logging ID for FSM is 201.

3 Minimum requirements and limitations

As mentioned earlier, the SAN Client and Fibre Transport components run on only a subset of the available Media Server and Client platforms. In addition, there are hardware and version requirements for both SAN Clients and Fibre Transport Media Servers. Before performing any troubleshooting on a SAN Client problem, you should verify that your Clients and Servers meet the SAN Client feature requirements.

3.1 Fibre Transport Media Servers

Fibre Transport Media Servers are supported on Solaris 9 and 10 on SPARC hardware, RedHat Enterprise Linux 4.0 and 5.0 on x86_64 hardware, and SUSE Linux Enterprise Server 9 service pack 2 on x86_64 hardware. In all cases, the 64 bit operating systems and server components must be installed.

The Fibre Transport Server requires at least one QLogic 2340, 2342, 2344, 2460, 2462, or 2472 Fibre Channel Host Bus Adapter. This adapter is required for the special Target Mode drivers used for the SAN transport of data between the Client and Server. Adapters used as Target Mode Fibre Transports can not be used for Tape or Disk connectivity. Other Host Bus Adapters (Initiator Mode) must be used to provide external Disk and/or Tape on the Server. The Initiator mode devices do not need to be QLogic Adapters, see the NetBackup Hardware Compatibility List for more details on supported Initiator Mode devices.

Finally it is suggested, for optimum performance, that all servers used for Fibre Transports have PCI-X or PCI-Express slots available for the Fibre Transport Target Mode adapters. See the performance considerations section for more details.

3.1.1 Solaris 9 and Solaris 10 Requirements

The Fibre Transport Services can be installed on Sun SPARC Sunfire servers running Solaris 9 or 10. Solaris 8 is not a supported Operating System for a Fibre Transport Media Server.

It is recommended that Solaris 10 update 7 or later be used on machines such as T5120/T5140 that have more than one IOMMU (see section 7.7).

3.1.2 RedHat Enterprise Linux 4 and 5 Requirements

The Fibre Transport Services can be installed on only the 64-bit RedHat 4 update 3, RH 4 update 5, RH 5 update 1, RH 5 update 2, or RH 5 update 3 releases for x86_64 processors. Furthermore, only the “ELsmp” kernel. The uniprocessor and “largesmp” kernels have not been validated for NetBackup 6.5.2 and later. The kernel mode drivers for the Fibre Transport require specific kernel versioning in order to install.

3.1.3 SUSE Linux Enterprise Server 9

Service pack 2 required.

3.2 SAN Clients

The SAN Client option is supported on most of the Tier 1 clients. Solaris, HP-UX, Linux, Windows, and AIX are all supported as SAN Clients with the exception of Windows on the Itanium platform (prior to NetBackup 6.5.4). In all cases, please refer to the NetBackup Hardware Compatibility List to verify Fibre Channel HBA compatibility for any particular platform.

3.2.1 AIX

AIX 5.1, 5.2, and 5.3 is supported on the pSeries platform for NetBackup 6.5. AIX has been verified using OEM IBM Fibre Channel adapters.

3.2.2 HP-UX

HP-UX 11.11, 11.23, and 11.31 is supported on the PA-RISC and IA64 platforms for NetBackup 6.5. See the Hardware Compatibility List for details on HBA supported for HP-UX. HP-UX relies on the pass-through driver, see the NetBackup Device Configuration Guide for detailed configuration information.

3.2.3 Linux

RedHat and SuSE Linux are supported as SAN Clients on 32bit and x86_64 platforms. Supported versions include SuSE 8.0, SuSE 9.0, RedHat 3.0, RedHat 4.0, and Redhat 5.0. Emulex and QLogic cards are supported using the OS native and HBA vendor drivers. Linux relies on the sg device driver for Tape Drive and SAN Client Fibre Transport communication. See the Linux section below for information on configuring the sg layer.

3.2.4 Solaris

Solaris 5.9 and 5.10 operating systems are supported on the SPARC and x86_64 platforms. Emulex and QLogic cards are supported using the OS native and HBA vendor drivers.

3.2.5 Windows

Windows 2000, 2003, and 2008 operating systems are supported on the 32bit and x86_64 platforms. Brocade, Emulex, and QLogic cards are supported using the HBA vendor drivers. Windows native drivers do not support transfers larger than 64k and SAN Client transfers are, by default, 256k. Brocade, Emulex, and QLogic supplied drivers are required for SAN Client transfers.

4 Fibre Channel Target Card marking (for FT Media Server usage)

In order to use a QLogic Fibre Channel port as a Fibre Transport Target, it must first be marked. Marking a card involves modifying the NVRAM on the QLogic HBA with a special value for the Subsystem Device ID. There are some potential pitfalls in marking a target port which should be avoided.

4.1 Marking cards on Solaris Servers

Solaris servers always require a reboot to load the card marking drivers.

4.2 Marking cards on QLogic 2312 and 24*xx* chipset system devices

First of all, and most importantly, you should not mark target ports on any Server with a system disk that resides on QLogic 2312 and 24*xx* chipset adapters. Setting up a system to mark cards installs a driver on every port that uses a 2312 or 24*xx* adapter, upon reboot the system disk will not be available.

4.3 Card marking when the system has active I/O on QLogic cards

If you start card marking on a system that has outstanding I/O on a QLogic card, you will have to skip unloading the QLogic drivers since they are busy. The 'nbhba' mode installer will require a reboot on a system that has active I/Os on QLogic cards. It should be noted that devices zoned to QLogic 2312 or 24*xx* chipset adapters will not be available while in 'nbhba' mode.

5 Installation Notes

5.1 Fibre Transport Media Servers

There are several configuration details during the installation of a media server which may affect the configuration of a Fibre Transport Media Server.

5.1.1 Media Server Naming Conventions

Verify that your naming conventions are consistent for Media Servers and Master Servers. If you use fully qualified names, use them for all your Fibre Transport media Servers, and if you use short names, be consistent in using short names for all your Media Servers as well.

5.1.2 Media Server Private Networks

Private networks are supported in NetBackup. If you use a Private Network as the secondary interface for Media Servers, you may need to create media server aliases in the EMM database.

5.2 SAN Clients

5.2.1 Installation of Private Branch Exchange

PBX is required for communications to the Master Server. PBX must be installed before the SAN Client service can complete startup.

5.2.2 Specifying a Master Server during installation

SAN Clients require communication to the EMM server for Fibre Transport operations. This requirement means that a SAN Client can only perform Fibre Transport operations within a single NetBackup domain. The client can allow Media Servers from outside the domain, but it can only communicate to a single instance of FSM.

5.2.3 Master Server Host Properties

The host properties for the Master Server can not contain “SERVER” entries for SAN Clients. The SAN Client can not be run on a Media Server, therefore if the client is given a SERVER entry, the SAN Client will shut down on that particular client. Server entries are typically added on Clients which have a Windows NetBackup Administrator Console.

5.2.4 Database SAN Clients

Database agents require that the NetBackup client is installed as the Database user. SAN Client backups write data to shared memory which is mirrored and transported to the Fibre Transport Media Server. Permissions on the shared memory require that the SAN Client is installed as the database user in order to take advantage of the shared memory. Backups and restores will fail without permission to write to the SAN Client shared memory.

5.2.5 Use WWPN in routed FC environments

HBA target ports in SANs in routed Fibre Channel environments must use the World Wide Port Name (WWPN) address. World Wide Node Name (WWNN) zoning will fail to discover Fibre Transport devices.

5.3 SAN Fabric Considerations

5.3.1 Inclusive Zoning

While all inclusive zoning is supported for SAN Client configurations, it is not recommended. An all inclusive zone runs a risk of a single misconfigured client or server affecting all the other SAN Clients in the zone.

5.3.2 Client Based Zoning

Zoning based on a client basis must contain all the Fibre Transport Servers to which the SAN Client will service.

5.3.3 Inter-Switch Links (ISL)

Whenever possible avoid using ISLs between SAN Clients and the Fibre Transport Media Servers with which they communicate. ISLs can quickly become congested when multiple transfers occur on multiple SAN Client Ports. Consolidate SAN Client zones on individual physical switches if possible.

Avoid Multi-Switch ISLs on all SAN Client transfers. In addition to increased latency, multi-switch hops consume double the available ISL bandwidth.

5.3.4 Reuse of SAN Client Fibre Channel Ports

San Clients can reuse the same SAN port for application data storage and SAN Client data transfers. There are performance considerations for doing such on both the application server and the SAN Client data transfer. The performance of such a configuration should be modeled to verify it will meet Service Level Agreements for the application server and the backup window.

5.3.5 Multiple SAN Client ports on a single SAN Client

The maximum number of Fibre Transport ports that will be used by a single SAN Client is equal to the number of SAN Client ports zoned to the Media Server. The port speed is not taken into consideration for the NetBackup 6.5.2 release. For example, a SAN Client can simultaneously use four Fibre Transport target ports for more than 700 MB/s of data transfer if the SAN Client has four ports zoned to the Media Server. If the SAN Client has only two ports zoned to the Media Server a maximum of two server ports will be used, even if the SAN Clients have available bandwidth to perform faster transfers.

6 Platform specific device configuration considerations

One benefit to using the SAN Client / Fibre Transport method to pool backup resources is that you can dynamically add high speed media servers when additional throughput is necessary for the pool of SAN Clients. In order to use the new Fibre Transport devices, you must discover the new devices through the SCSI layer on the SAN Client. Most of the SAN Clients supported for NetBackup 6.5 have mechanisms to add SCSI devices (hotplug) without requiring a reboot.

In all cases, the SAN Client service will require a rescan through the GUI or the CLI (nbftconfig -rescan) to update FSM with the new devices.

6.1 AIX

An AIX SAN Client using the native Fibre Channel drivers can discover Fibre Transport Targets without requiring a reboot. On AIX run 'cfgmgr' with no arguments to perform device discovery. You can run 'lsdev -Cc tape' to list the tape devices known to the SAN Client.

6.2 HP-UX

A HP-UX SAN Client can discover Fibre Transport Targets without requiring a reboot. Use 'ioscan -fnC stape' and 'insf -e' at the command line to initiate Fibre Channel Discovery and create device files for newly discovered devices.

HP-UX servers rely on the SCSI pass through driver for SAN Client transfers. Devices need to be created in the /dev/sctl directory before the SAN Client can use them. Specifics for creating these devices is found in the NetBackup Device Configuration Guide.

6.3 Linux

The Linux sg device layer does not perform discovery beyond LUN 0 by default. Since the Fibre Transport server presents two LUNs on a single target you must add sg devices for the second LUN to take advantage of the second Fibre Transport device. The command used in Linux to manually add sg devices looks like the following:

```
echo "scsi add-single-device H C T 1"    >
/proc/scsi/scsi
/dev/MAKEDEV sg
```

The target value **H** should be replaced by a host value. Typically you would add entries for all the Fibre Transport servers in the SAN.
The target value **C** should be replaced by a channel value. Typically you would add entries for all the controllers in the system.
The target value **T** should be replaced by a target value. Typically you would add entries for targets 0-7 at a minimum.
The MAKEDEV directive creates any necessary device files to support the newly added devices.

Linux clients using 2.4 kernels may require a reboot to discover new devices out on the SAN. Linux 2.6 kernels can, in most cases, use the above procedure to discover new devices on the SAN without a reboot. For a rescan to occur, you need to create a script that performs echoes to /proc/scsi/scsi for each device on the SAN.

6.4 Solaris

A Solaris SAN Client using the native Fibre Channel drivers can discover Fibre Transport Targets without requiring a reboot. On Solaris you can run 'cfgadm -al' to list all the available Interfaces on the system. From here you can determine what interface is connected to the SAN Client fabric and run a 'cfgadm -c configure *node*' to create device entries for the Fibre Transport devices.

Solaris requires entries in the /kernel/drv/st.conf to discover any devices above LUN 0 on a SCSI target. Since the Fibre Transport server presents two LUNs on a single target you must add entries for the second LUN to take advantage of the second Fibre Transport device. Each entry is of the form:

```
name="st" class="scsi" target=X lun=1;
```

The target value X should be replaced by a target value. Typically you would add entries for targets 0-7 at a minimum.

6.5 Windows

The default drivers installed for QLogic Fibre Channel adapters do not support block sizes larger than 64k. Fibre Transport servers default to 256k transfers, so data transfers will fail using the default drivers. Install device drivers from the HBA vendor in order to support large transfers.

Windows SAN Clients do not require Tape Drivers for discovered Fibre Transport devices. If the Windows SAN Client discovers "Archive Python" devices it will place them under "Unknown Devices" in the Device Manager. When this occurs, the Windows SAN Client will write data directly to the SCSI port rather than the Tape Class driver. If Tape Drivers are installed, then the data will take advantage of the tape device driver.

Windows SAN Clients can discover tape devices without requiring a reboot. Usually rescanning devices in the Device Monitor will display new devices on a SAN Client. If the Device Manager fails to discover newly added devices, the software provided by the HBA vendor can be used to initiate discovery. If the vendor utilities are not installed, the Fibre Channel cable to the HBA port can be removed and replaced to initiate Fibre Channel discovery. If you have no physical access to the machine, a reboot may be necessary.

If using the Storport SCSI driver, be sure to apply an updated Storport from Microsoft available at: http://support.microsoft.com/kb/903081

7 Troubleshooting

The following section provides some hints to fix some common problems found with the SAN Client feature. In this section we list some common problems as well as a list of steps to take which can help fix some common errors in the installation or configuration of the SAN Client feature.

7.1 The SAN Client service does not start up.

- ***Is the Private Branch Exchange (PBX) service installed and running?***
  If you list the processes "bpps -x" there should be a process running called "pbx_exchange"
- ***Is the Client configured as a SAN Client?***
  Run the 'bpclntcmd -sanclient' to return the current state of the SAN Client. A response of '0' indicates that SAN Client is not configured, rerun the command with 'bpclntcmd -sanclient 1'
- ***Is the client also a Media, Master, or EMM server?***
  The SAN Client process will not run on anything but a NetBackup Client.

- ***Is there a valid license for the SAN Client feature on the Master Server?***
  SAN Client is a separately licensed feature which requires a key called "SAN Client" on the Master Server.
- ***Are there Server entries for the SAN Client on the Master Server?***
  Remove any 'SERVER=clientname' entry in the Master Server for the SAN Client. If the Master Server believes the SAN Client is also a Server, it might shutdown the SAN Client.
- ***Have you restarted the Client Service?***
  Although the SAN Client will be started on reboots of a server, it will not automatically start up after you run the 'bpclntcmd' command. You must run the client startup script, or use the Service Manager in Windows, to start the SAN Client service.

7.2 The Fibre Transport services does not start up

- ***Are there any marked QLogic Target ports in the server?***
  The 'nbftsrvr' and 'nbfdrv64' processes will exit if the system has no ports available for Target Mode use.
- ***Is there a valid license for the SAN Client feature on the Master Server?***
  SAN Client is a separately licensed feature which requires a key called "SAN Client" on the Master Server. The Fibre Transport server performs a license check during startup.
- ***Was a reboot required for the installation of the Fibre Transport Server?***
  All Solaris installations require that the Media Server be rebooted after the install of Fibre Transport in order to load the Fibre Transport drivers on the marked target ports. In addition, Linux servers need to be rebooted if you elected to not unload the existing QLogic drivers during the installation of Fibre Transport.

7.3 My SAN Client is not discovering devices from my Fibre Transport Servers

- ***Is your Fibre Transport Server running?***
  SAN Clients can not discover the devices from a Fibre Transport server unless the service is running on the Media Server. Verify the 'nbftsrvr' and 'nbfdrv64' processes are active on the Media Server.
- ***Are your Clients and Servers properly zoned?***
  Use the SAN Fabric configuration software to verify that your SAN Clients and the Fibre Transports they use are contained in the same zone. Verify that all the respective ports are online.
- ***Have you followed the Fibre Channel discovery techniques outlined in section 6?***
  There are several different configuration steps necessary for performing Fibre Channel Discovery on an Operating System level. Please view the

NetBackup Device Configuration Guide as well as documentation for your Operating System for more in-depth information in these steps.

- ***Are any Fibre Transport devices logged in the SAN Client startup?***
  The logging for the SAN Client feature 'vxlogview -i 200 -o 200' can provide insights into the devices a SAN Client has discovered. If you scan the logs for the SAN Client, you should be able to view all the devices it has discovered as well as the Media Servers that present those devices. Verify that the Media Server names in the logging match those used by NetBackup. If there is an disparity between the names, you will need to create an EMM alias for the name displayed in the SAN Client logs to the one configured for the Media Server.

7.4 My jobs are not using Fibre Transport

- ***Is your naming convention consistent?***
  The name used for your SAN Client install should be the same as the name used in the policy. In addition, your Media Servers should be consistently named with either short names or fully qualified names.
- ***Are you using Multiple Copies?***
  Multiple copies are not supported on backup because of the performance considerations inherent in having multiple mixed speed destinations. Disable Multiple Copies for any policy that requires Fibre Transports.

7.5 My performance is slower than expected

- ***What speed are your Fibre Transport Target cards running at?***
  There are some specific circumstances that can downshift the bus speed of PCI-X slots below the speeds stated in the System Documentation. During the initialization of the Fibre Transport, the bus speed of each port is displayed in the Logging for the Fibre Transport. Look for lines containing "InitializeSDC"
  `vxlogview -i 199 -o 199 | grep InitializeSDC`
  Ideally a four port Fibre Transport card requires a 133mhz PCI-X slot, a two port card should use a 100mhz PCI-X slot, and a single port card could use a 66mhz slot.
- ***Are you using Switch ISLs for Fibre Transport communications?***
  The Fibre Transport option can place a heavy burden on Inter Switch Links (ISL) in a fabric. You should have trunking options enabled for multi-fibre ISLs, and you should always make certain that your ISLs are not oversubscribed for the data transfers required.
- ***Are your backend storage units capable of reading and writing to support the transfer?*** In order to transport at high data rates between servers and clients we have to verify that the entire infrastructure from Client to Server is capable of meeting a performance target. For example, an 8 stream backup of an Oracle database requires that the client reads 8

simultaneous streams of data from its disks, that the same 8 streams of data are transported across the SAN, and finally that they are written simultaneously to the Server disk. Each one of those steps should be profiled.

- ***Do you have available processor time?***
  Transporting data at high speeds from the frontend disks to a backend Fibre Transport requires a non-trivial amount of CPU usage. For example, a 600 MB/s Fibre transfer on a Linux 64 bit client requires 1.2 GB/s of system I/O to both read from the application disks and write to the Fibre Transport. This can consume almost 3ghz of the system's processors. If the Fibre Transport service has to compete with an application for processor cycles, it may have an impact on performance.

7.6 SAN Client service can not start in a timely manner on Windows SAN Clients.

On some Windows configurations, the default service timeout of 30 seconds is insufficient time for SAN Client to initialize and load. Specifically, when a system has many large boot time services or has limited resources, the client may timeout and fail to start the "SAN Client Fibre Transport Service" When this occurs, back ups cannot use Fibre Transport unless the client is started manually.

To workaround this timeout, increase the timeout to a value that gives the SAN Client service enough time to startup. In the Windows registry of the SAN Client, edit the following key:

```
\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
ServicesPipeTimeout
```

This key describes the service timeout in milliseconds. Set the value to REG_DWORD = 90000, which increases the timeout to 90000 milliseconds.

7.7 My Solaris FT media server does not use all of the target mode cards.

On Solaris systems (prior to 10 update 7), NetBackup 6.5.2 and later detect the PCI bus and only allow ports on one bus to be used for target mode, as follows:

- 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.

7.8 I've updated my NetBackup release but I can't use new Fibre Transport features.

If the Fibre Transport server was installed prior to the NetBackup update, drivers for the new release must be reinstalled in the operating system driver directories.

To complete your update for Fibre Transport you must first uninstall the Fibre Transport `/usr/openv/netbackup/bin/admincmd/nbftsrv_config -d' then reinstall the drivers with `/usr/openv/netbackup/bin/admincmd/nbftsrv_config' A reboot will be necessary on the Solaris platform.

7.9 My HBA in Target Mode does not login to Fabric Switch.

In NetBackup releases 6.5 to 6.5.2, the target mode driver on Fibre Transport media servers only works in L-Port mode. The fabric switch must support L-Port logins for target mode HBAs.

This applies to all HBA firmware variants we support – ISP2312, ISP2422 and ISP2432.

7.10 Inappropriate FT media server shutdown can cause the server to hang

The NetBackup media server shutdown scripts that stop the Fibre Transport nbftsrvr and nbfdrv64 processes gracefully. "Gracefully" includes stopping the QLogic HBA ISP chip sets that are in target mode.

In some random circumstances, sufficient time for the shutdown processing may not be allowed. A system reboot may hang. For example, operating system restart procedures on the Red Hat 5 and SLES 10 releases may have altered the allowed time between SIGTERM and SIGKILL or changed the RC shutdown script processing. In such cases, the ISP chip set can have outstanding DMA activities or Fibre Channel events can trigger alteration of the memory previously allocated by nbfdrv64 for communication with the ISP chip sets.

Symptoms of this kind of failure are usually system hangs that are unresponsive to anything but a power off and rarely leave any clues in the system log; any clues left are not specific to this problem and are more an indication of memory corruption. The system hang may be accompanied by a multi-colored video display pattern (a strong indication of this kind of failure).

The only known resolution is to power cycle the machine, leaving the power off long enough for all power indications to go off (and thus stop the run away QLogic ISP chip sets).

This issue occurs on NetBackup 6.5 and later and NetBackup 7.0 and later on some Red Hat 5 and SLES 10 Linux machines.

8 Revision history

Revision A Added a Windows troubleshooting item.

Revision B Changes for NetBackup 6.5.2.

Revision C Added information about World Wide Node Names in multiple SAN, routed environments.

Revision D Added Brocade as a supported HBA for SAN clients.

Revision E Platform proliferations.

Revision F Added a troubleshooting item about inappropriate FT server shutdown.