Veritas NetBackup™ Appliance iSCSI Guide

VERITAS™

Veritas NetBackup™ Appliance iSCSI Guide

Documentation version: 3.0

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

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

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

www.veritas.com/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.veritas.com/support

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Technical Support
  - Recent software configuration changes and network changes

Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Contents

Chapter 1

Overview

This chapter includes the following topics:

About iSCSI

iSCSI is a way of connecting storage devices over a network by using TCP/IP. iSCSI was developed to enable transmission of SCSI commands over the existing Internet Protocol (IP) network by using the TCP/IP protocol. iSCSI offers the possibility of delivering both messaging traffic and block-based storage over IP networks without installing a separate Fibre Channel network. With release 3.0, iSCSI supports VMware backups on configuration H of the NetBackup 5240 appliance.

The protocol allows clients (called initiators) to send SCSI commands to SCSI storage devices (targets) on remote servers. Configuration H of the NetBackup 5240 appliance functions as an initiator.

A target is a storage resource located on an iSCSI server (more generally, one of the potentially many instances of iSCSI storage nodes running on that server). To communicate with each other, iSCSI initiators and targets establish iSCSI sessions

About iSCSI initiator and targets

iSCSI is a way to share storage over a network and works at the block device level. For iSCSI communication, the following components talk with each other:

- Initiator
- Target

The clients which access the iSCSI storage are called initiators. This iSCSI Initiator can connect to a server (the iSCSI target). In doing so, the iSCSI Initiator sends SCSI commands to the iSCSI target. These SCSI commands are packaged in IP packets for this purpose.

An iSCSI target device receives iSCSI commands and shares the storage. The storage can be a physical disk, or an area representing multiple disks or a portion of a physical disk. A storage array is a typical iSCSI target.

Supported iSCSI features

See the following pointers to understand how iSCSI is supported with NetBackup appliances:

- iSCSI is supported only on configuration H of the 5240 appliance.
- Configuration H of the NetBackup 5240 appliance always functions as an initiator.
  See "NetBackup 5240 Appliance configuration H" on page 13.
- iSCSI supports VMware backups only. It supports the NetBackup for VMware feature.
  See "About NetBackup for VMware" on page 17.
- For this release, the iSCSI functionality (commands) are available on the NetBackup Appliance Shell Menu only.
- iSCSI supports IPv4 addresses only. iSCSI connections over IPv6 are not supported.
  In addition, the initiator and the target must be on the same Layer 2 network (L2).
- iSCSI supports Dynamic Multi-Pathing (DMP). You can connect via multiple paths to the same target. The backups or restores over iSCSI can continue as long as one path is available.
- A VLAN can be configured on either the network interface or the iSCSI interface. If VLAN is configured on both the network and iSCSI interface, the VLAN for the network interface is effective on both the interfaces. Note that when VLAN

is configured on both the network and iSCSI interface on different subnets, the configuration is not supported.

Network Interface		iSCSI Interface		Description
IP	**VLAN**	**IP**	**VLAN**	
Subnet X	None	Subnet X	None	Supported
Subnet X	None	Subnet Y	VLAN A	Supported
Subnet X	VLAN B	Subnet X	VLAN B	Supported
Subnet X	VLAN B	Subnet Y	VLAN B	Not Supported

- Using an iSNS server (Internet Storage Name Service) for discovering targets is supported.
  See "About iSNS" on page 28.
- Only a QLogic Small Form-Factor Pluggable (SFP+) module is supported in the 10Gb Ethernet/iSCSI card. You will receive an alert if an unsupported SFP module is detected in the 10Gb Ethernet/iSCSI card (if alerts are configured).

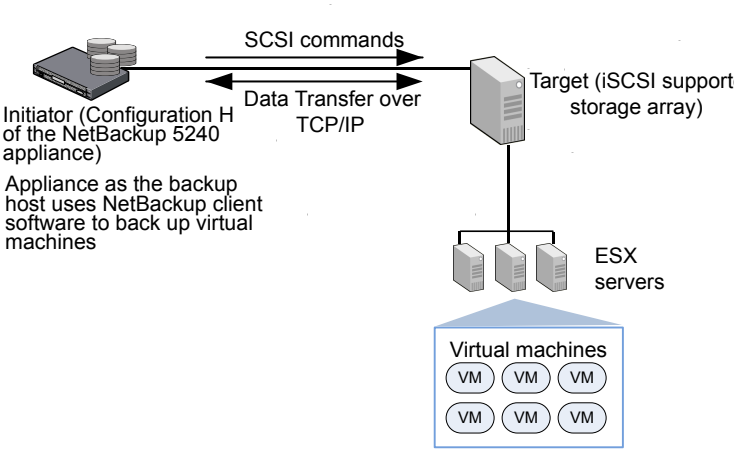
For the latest NetBackup Appliance compatibility information, refer to the Hardware Compatibility List on the following website:

www.netbackup.com/compatibility

Overview of the iSCSI topology

The appliance can operate as the VMware backup host and take VMware backups by using iSCSI. In this topology, the appliance functions as an initiator and is connected to a storage array (target) on a TCP/IP network. The storage array can be connected to an ESX host over FC/LAN etc.

Figure 1-1 iSCSI topology



The virtual machines are backed up on the appliance over iSCSI.

About the iSCSI Qualified Name (IQN)

In an iSCSI network, each iSCSI element that uses the network has a unique iSCSI name and is assigned an address for access. Each iSCSI element, whether an initiator or target, is identified by a unique iSCSI Qualified Name (IQN). The IQN is a logical name that is not linked to an IP address.

The IQN has the following properties:

- It is unique. No two initiators or targets can have the same name.
- It can be up to 255 characters long.
- It can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), and periods (.).

A sample IQN format is `iqn.yyyy-mm.naming-authority:unique name` where:

- `yyyy-mm` is the year and month when the naming authority was established.
- naming-authority is usually reverse syntax of the Internet domain name of the naming authority.
- Unique name is any name you want to use, for example, the name of your host. The naming authority must make sure that any names assigned following the colon are unique.

Example: iqn.1999-06.com.veritas:abc

Chapter 2

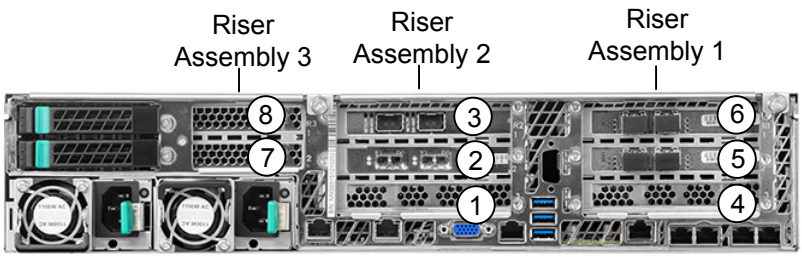
Understanding the NetBackup 5240 appliance configuration H

This chapter includes the following topics:

NetBackup 5240 Appliance configuration H

The rear panel of the NetBackup 5240 Appliance contains three PCIe riser card assemblies. PCIe riser card assemblies 1 and 2 each support three standard PCIe cards, while PCIe riser card assembly 3 supports two low profile PCIe cards. The slots are labeled 1 to 8. Slots 1, 2, and 3 are located in PCIe riser card assembly 2. Slots 4, 5, and 6 are located in PCIe riser card assembly 1, while slots 7 and 8 are located in PCIe riser card assembly 3.

Figure 2-1 Rear panel riser assembly locations and PCIe slot assignments for configuration H



The NetBackup 5240 Appliance supports multiple PCIe-based I/O configuration options. The following table shows the configuration H option that has the iSCSI card in slot 2.

Table 2-1 NetBackup 5240 Appliance configuration H

I/O configuration option	Slot 1 *	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7 **	Slot 8
H	-	10 GbE NIC [1, 3] (iSCSI)	10 GbE NIC [1, 3]	-	8 Gb FC HBA [3]	8 Gb FC HBA [3]	-	-

* Slot 1 contains a factory installed PCIe RAID 6 controller when at least one NetBackup 5240 Storage Shelf is purchased with the NetBackup 5240 Appliance. Otherwise, slot 1 is not populated.

** Slot 7 contains the NetBackup 5240 Appliance's internal PCIe raid controller. This RAID controller is used to create the RAID 1 Array for the disk drives on which the appliance operating system is installed. The operating system drives are located in slots 0 and 1 of the front panel.

PCIe card cable connection types:

[1] Direct-Attach copper cable (also called a Twinaxial cable or Twinax)

[2] Standard copper cable

[3] Fiber optic cable

See the *NetBackup Appliance Product Description Guide* for more details.

QLE8442 dual-port 10Gb Ethernet/iSCSI capable card

The QLE8442 dual-port 10GbE is an iSCSI capable card that is available with configuration H of the NetBackup 5240 appliance.

It supports the iSCSI protocol at 10Gb Ethernet (10GbE) line rate. The card provides iSCSI hardware offload, which reduces CPU-intensive iSCSI protocol processing.

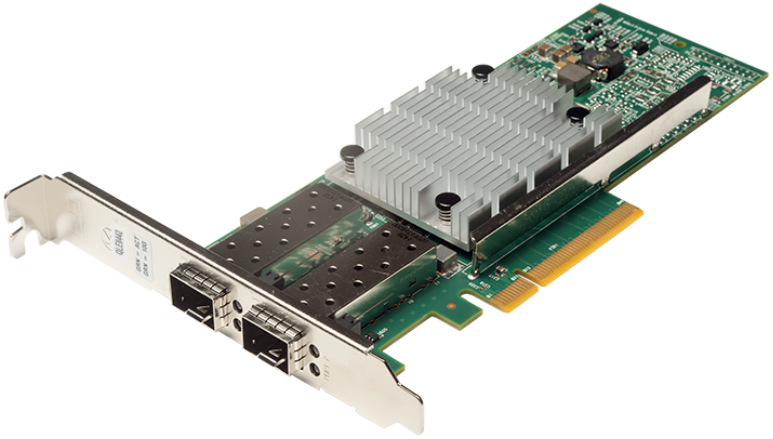


Table 2-2 QLE8442 dual-port 10Gb Ethernet card specifications

Item	Specification
Bracket height	Full height
Power consumption	9.65 watts (nominal)
System interface type	PCIe v3.0
Speed and slot width	8.0 GT/s, 8-lane
Storage over Ethernet	iSCSI
LED indicators	LINK/ACTIVITY Off = No link (cable disconnected) Continuously illuminated = Line on Blinking = Network activity
Certifications	FCC A, ICES A, UL, CE, VCCI, CISPR, KCC
Operating temperature	0 to 55 C (32 TO 131 f)
Storage temperature	-40 to 65 C (-40 to 149 F)
Operational humidity	7% to 93% @ 55 C

Table 2-2 QLE8442 dual-port 10Gb Ethernet card specifications *(continued)*

Item	Specification
Storage humidity	93% maximum at 65 C
Air flow	100 LFM @ 55 C

Chapter 3

Understanding NetBackup for VMware

This chapter includes the following topics:

About NetBackup for VMware

NetBackup for VMware provides backup and restore of the VMware virtual machines that run on VMware ESX servers. NetBackup for VMware takes advantage of VMware vStorage APIs for data protection. The backup process is off-loaded from the ESX server to a VMware backup host.

NetBackup for VMware does the following:

- Performs off-host backup of virtual machines (NetBackup client software is not required on the virtual machine). Off-host backup reduces the backup processing load on the VMware host.
- Increases the backup speed as compared to standard file-order backup methods, if the virtual machine is heavily populated with small files.
- Automatically creates quiesced snapshots using VSS (Windows only). Creates the quiesced snapshots on Linux if the SYMCquiesce utility is installed.
- Uses snapshot technology to keep virtual machines 100% available to users.
- Supports VMware vSphere and vCloud Director.
- Performs full backups and incremental backups, including block-level incrementals.

- Backs up the full virtual machine.
- Backs up the virtual machines even when they are turned off.
- Can restore selected files from the backup.

Overview of the VMware backup process

The following table describes the phases in the NetBackup backup process.

Table 3-1 NetBackup backup process

Phase	Description
Phase 1	The NetBackup master server initiates the backup.
Phase 2	The NetBackup client on the VMware backup host initiates a VMware snapshot on the virtual machine.
Phase 3	Windows: VSS synchronizes the file system on the virtual machine. Linux: The SYMCquiesce utility can quiesce the file system on supported Linux operating systems.
Phase 4	The VMware server creates a snapshot on the virtual disk datastore.
Phase 5	The NetBackup client reads the snapshot from the datastores and writes the data to the NetBackup storage unit.

Transport modes options (VMware)

The transport modes determine how the snapshot data travels from the VMware datastore to the VMware backup host. The appropriate mode depends in part on the type of network that connects the VMware datastore to the VMware backup host.

By default, all modes are selected. NetBackup tries each transport mode in order, from top to bottom. It uses the first mode that succeeds for all disks in the virtual machine.

Table 3-2 Transport Modes

Mode	Description
san	For unencrypted transfer over Fibre Channel (SAN) or iSCSI. **Note:** On NetBackup appliances, the VMware backups happening over iSCSI use the **san** transport mode. **Note:** This mode is not supported for the virtual machines that use VMware Virtual Volumes (VVols).
hotadd	Lets you run the VMware backup host in a virtual machine. **Note:** For the virtual machines that use VVols, the virtual machine and the backup host (hotadd) virtual machine must reside on same VVol datastore. For instructions on this transport mode and on installing the backup host in a VMware virtual machine, refer to your VMware documentation.
nbd	For unencrypted transfer over a local network that uses the Network Block Device (NBD) driver protocol. This mode of transfer is usually slower than Fibre Channel.
nbdssl	For encrypted transfer (SSL) over a local network that uses the Network Block Device (NBD) driver protocol. This mode of transfer is usually slower than Fibre Channel.

Chapter 4

Configuring iSCSI

This chapter includes the following topics:

Configuring the appliance for iSCSI

Before configuring your appliance for iSCSI, ensure that the iSCSI targets are configured in your environment. Check the documentation provided by the target vendor for more reference.

Table 4-1 provides instructions to configure and set up iSCSI on the appliance.

Table 4-1 Configuring iSCSI on the appliance

Step No.	Description	Reference
1.	Configure IQN for the initiator	See "Setting the IQN for the initiator" on page 21.
2.	Configure the iSCSI interface. The IP address must be configured. You may optionally configure other interface properties like Netmask, gateway etc.	See "Configuring the interface properties" on page 22.
3.	Discover the targets by using the portal address or the iSNS server.	See "Discovering targets by using the portal address" on page 27. See "Discovering targets by using iSNS" on page 29.
4.	Connect to the target	See "Connecting to a target" on page 31.

Setting the IQN for the initiator

This section explains how you can set the IQN for the NetBackup Appliance (initiator).

To set the IQN

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.
3. Type the command **Initiator Set IQN** and enter the IQN as a parameter.

   Note the following about IQN:

   - The IQN must be up to 255 characters long.
   - The IQN can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), and periods (.).

   Example: iqn.1999-06.com.veritas:abc
4. The following message is displayed:

```
iSCSI> Initiator Set IQN iqn.veritas.abc
- [Info] The IQN has been updated to iqn.veritas.abc.
```

Viewing the interface properties

This section lists the procedures for viewing the iSCSI interface properties.

To view the interface properties

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.
3. Type the command **Interface Show** and press **Enter** to view the iSCSI interfaces. The following properties are displayed:

```
appliance.iSCSI > Interface Show
Showing the available interfaces...

+--------------+----------+-----------------+-------------+-------+-------+----+----+
|Interface Name|Network   |   MAC Address   | IP Address  |Netmask Gateway|MTU |VLAN
|              |Interface |                 |             |       |       |    |Tag |
+--------------+----------+-----------------+-------------+-------+-------+----|----+
|     iscsi1   |  eth6    |00:0e:1e:53:55:11|10.181.198.62|       |       |1500|    |
+--------------+----------+-----------------+-----------|-------------+-------+----+----+
|     iscsi2   |  eth7     |00:0e:1e:53:55:13|           |       |       |1500|    |
+--------------+----------+-----------------+-----------|-------------+-------+----|----+
```

Configuring the interface properties

This section lists the procedures for configuring interface properties like gateway, IPv4 address, Netmask, Maximum Transmission Unit (MTU), and the VLAN Tag for an ISCSI interface.

The MTU controls the maximum transmission unit size for an Ethernet frame. It must be a number from 68 to 65535. Note that when you configure the MTU for an iSCSI interface, the new MTU value is configured for both the iSCSI interface and the network interface to which it is mapped.

VLAN Tagging is the practice of inserting a VLAN ID into a packet header in order to identify which VLAN (Virtual Local Area Network) the packet belongs to. More specifically, switches use the VLAN ID to determine which ports, or interfaces, to send a broadcast packet to.

A VLAN can be configured on either the network interface or the iSCSI interface. If VLAN is configured on both the network and iSCSI interface, the VLAN for the network interface is effective on both the interfaces.

To configure the IP address

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.
3. Type the command **Interface IPAddress Set**.
4. Enter the IP address and the iSCSI interface name as parameters. Press **Enter**.

   Example:

```
iSCSI> Interface IPAddress Set 10.80.156.88 iscsi1

[Info] The IP address has been configured for iscsi1.
```

Note: The values used in the examples are sample placeholder values.

To configure the Netmask

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.
3. Type the command **Interface Netmask Set**.
4. Enter the Netmask value and the iSCSI interface name as parameters. Press **Enter**.

   Example:

```
iSCSI> Interface Netmask Set 255.255.255.0 iscsi10

[Info] The Netmask has been configured for iscsi10.
```

To configure the gateway

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.

3 Type the command **Interface Gateway Set**.

4 Enter the gateway value and the iSCSI interface name as parameters. Press **Enter**.

Example:

```
iSCSI> Interface Gateway Set 192.168.4.1
   iscsi10

[Info] The gateway has been configured for iscsi10.
```

To configure the Maximum Transmission Unit (MTU)

1 Open a Secure Shell (SSH) session to log on to the appliance as an administrator.

2 Navigate to the **Main_Menu > Settings > iSCSI** menu.

3 Type the command **Interface MTU Set**.

4 Enter the MTU value and the iSCSI interface name.

The MTU must be a number from 68 to 65535. The new MTU value applies to the iSCSI interface and also the network interface that it maps to.

Example:

```
iSCSI> Interface MTU Set 3000 iscsi10

The new MTU value applies to both iscsi1 and
also network interface eth6.
Do you want to continue?(yes/no)[no]:yes

[Info] The MTU has been configured for iscsi10.
```

To configure the VLAN tag

1 Open a Secure Shell (SSH) session to log on to the appliance as an administrator.

2 Navigate to the **Main_Menu > Settings > iSCSI** menu.

3 Type the command **Interface VLAN Set**.

4 Enter the VLAN ID and the iSCSI interface name as parameters. Press **Enter**.

The VLAN ID must be a number from 1 to 4095.

Example:

```
iSCSI> Interface VLAN Set 75 iscsi10

[Info] The VLAN tag has been configured for iscsi10.
```

Removing and resetting the interface properties

This section lists the procedures for removing all the interface properties except MTU. It also contains the procedure to reset MTU to the default value (1500).

The MTU cannot be removed and can only be reset to its default value.

To remove the interface properties

1 Open a Secure Shell (SSH) session to log on to the appliance as an administrator.

2 Navigate to the **Main_Menu > Settings > iSCSI** menu.

3 Use the following commands to remove the specific properties:

- Type the command **Interface Gateway Remove** and enter an iSCSI interface name.
  This command removes the gateway from the specified interface.
  Example:

  ```
  iSCSI> Interface Gateway Remove iscsi1

  [Info] The Gateway has been removed from iscsi1.
  ```

- Type the command **Interface IPAddress Remove** and enter an iSCSI interface name.
  The command removes the IP address from the specified interface.
  Example:

  ```
  iSCSI> Interface IPAddress Remove iscsi1

  [Info] The IP address has been removed from iscsi1.
  ```

- Type the command **Interface Netmask Remove** and enter an iSCSI interface name.

The command removes the Netmask from the specified interface.
Example:

```
iSCSI> Interface Netmask Remove iscsi1

[Info] The Netmask has been removed from iscsi1.
```

- Type the command **Interface VLAN Remove** and enter an iSCSI interface name.
  The command removes the VLAN tag from the specified interface.
  Example:

```
iSCSI> Interface VLAN Remove iscsi1

[Info] The VLAN tag has been removed from iscsi1.
```

To reset the MTU

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.
3. Type the command **Interface MTU Reset** and enter an iSCSI interface name. Note that the command resets MTU to the default value (1500) on both the iSCSI interface and the network interface to which it maps.

   Example:

```
iSCSI > Interface MTU Reset iscsi1
The MTU will be reset to 1500 for both iscsi1 and also
the network interface eth6.
Do you want to continue?(yes/no)[no] :yes

[Info] The MTU has been reset to 1500.
```

About CHAP authentication

The authentication method that is used for appliances is called Challenge Handshake Authentication Protocol (or CHAP). The CHAP authentication can be applied to the following commands or actions:

- Discovering a target
- Connecting to the target

During the initial stage of an iSCSI session, the appliance (initiator) sends a login request to the storage system to begin an iSCSI session. The storage system will then either permit or deny the login request, or determine that a login is not required. If authentication is enabled on the target, the credentials must be authenticated and the session established before the server can access the storage resources. The server compares the value from the client and, if the information matches, grants the session. If the response fails, the session is denied, and the request phase starts over.

The initiator logs in using a CHAP user name and password. You can specify a CHAP password or generate a random password. To set up and configure CHAP authentication, see the target vendor documentation.

Discovering targets by using the portal address

This section provides instructions for discovering iSCSI targets by using the target portal address. The target portal address is the hostname or IPv4 address that is associated with the target.

The format of the target portal address is **<IPv4 Address/hostname>:[<port>]**.

Example: 192.116.116.50 or abc:3260 where 3260 is the default port.

You must first discover a target in order to connect to it.

To discover a target by using the target portal address

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the Main_Menu > Settings > iSCSI menu.
3. Type the command **Target Discover Portal**
4. Enter the target portal address and the iSCSI interface name that you have configured as parameters. Note the following considerations:
   - The target portal address must be of the following format: **<IPv4 address/hostname>[:port]**. The host name can be a short name or a fully qualified domain name.
     Example: 192.116.116.50 or abc:3260

- The iSCSI interface name can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), under scrores (_) and periods (.) It must begin with numbers (0-9), letters (A-Z and a-z) and underscores (_) only.

5 Run the **Target Discover Portal <Portal Address> <Interface Name>** command. You are asked to provide a username and password. Type **yes** if your target requires authentication. The targets that are available on the specified portal address and interface are discovered and displayed in the following manner:

```
Does your target require a username and password? (yes,no)[no]:no

Showing the discovered targets...

+-----+------------------------|---------------------|----------------+
| No. |     Target IQN         |Target Portal Address|   Interfaces   |
+-----+------------------------|---------------------|----------------|
|  1  |iqn.1996-03.veritas:abc | 10.121.98.22:3260   | iscsi1, iscsi2 |
+-----+------------------------|---------------------|----------------|
|  2  |iqn.1996-03.veritas:xyz | 10.121.98.23:3260   | iscsi1, iscsi2 |
+-----+------------------------|---------------------|----------------+
|  3  |iqn.1996-03.veritas:host| 10.121.98.24:3260   | iscsi1, iscsi2 |
------|------------------------|---------------------|----------------|
```

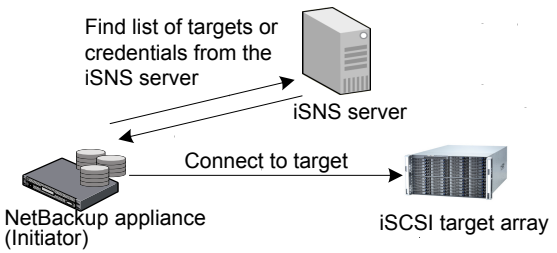
Note: If you run the `iSCSI > Target Discover Portal` or `iSCSI > Target Discover iSNS` command again after the targets are connected, it overrides the existing connection settings like target credentials. If the target requires authentication, you will need to enter the target credentials again when the existing sessions are reconnected. The existing sessions need to be reconnected if the appliance restarts or when you change the IQN for the appliance or when the iSCSI processes are restarted etc.

About iSNS

An iSNS server uses the Internet Storage Name Service protocol to maintain information about active iSCSI devices on the network, including their IP addresses, iSCSI node names, and portal groups. The iSNS protocol enables automated discovery and management of iSCSI devices on an IP storage network. An iSCSI initiator like the NetBackup appliance can query the iSNS server to discover iSCSI target devices.

You can use an iSNS (Internet Storage Name Service) server to discover targets. Configuring the iSNS server eliminates the need for configuring every initiator for every target. When numerous hosts exist on a network, configuring an iSNS server saves time. An iSNS server provides a central management point for the group by dynamically maintaining up-to-date information about the iSCSI target names for group volumes.

If you are using an iSNS server, there is no need to discover targets by using the specific target names in the command. The following diagram explains the interaction between the appliance and the iSNS server.



Discovering targets by using iSNS

This section provides instructions for discovering iSCSI targets by using the Internet storage name service (iSNS) method. Use this method if you have at least one iSNS server on your network. This method enables the iSCSI initiator to discover targets that are registered to the iSNS server. For this method, you must supply the iSNS server address and/or port. The iSCSI initiator can then query the specified iSNS server to discover targets. The default port for an iSNS server is 3205.

You can connect to a target only after discovering it. Review the following considerations:

- If you run the `iSCSI > Target Discover Portal` or `iSCSI > Target Discover iSNS` command again after the targets are connected, it overrides the existing connection settings like target credentials. If the target requires authentication, you will need to enter the target credentials again when the existing sessions are reconnected. The existing sessions need to be reconnected if the appliance

restarts or when you change the IQN for the appliance or when the iSCSI processes ae restarted etc.

- When targets are discovered by using iSNS on two iSCSI interfaces like first run the `Target Discover iSNS` command for *iscsi1* and then *iscsi2*, only the recent record is displayed by the `Target Show All` command. For example the **Interfaces** column in the `Target Show All` command may not show both the interfaces (*iscsi1*, *iscsi2*) for some targets. It actually shows the interface from the most recent command (*iscsi2* in this case) for some targets.

To discover iSCSI targets by using an iSNS server

Note: An iSNS server must already be set up and available on the network before running the following procedure.

---

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the Main_Menu > Settings > iSCSI menu.
3. Type the command **Target Discover iSNS**.
4. Enter the address of the iSNS server and the iSCSI Interface name that you have configured as parameters.
   - The iSNS address must be of the following format <IPv4 address/hosname>[:port]. The host name can be a short name or a fully qualified domain name. The default port is 3205.
     Example: 192.116.50.50 or abc:3205

- The iSCSI interface name can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), under scrores (_) and periods (.) It must begin with numbers (0-9), letters (A-Z and a-z) and underscores (_) only.

5 Run the **Target Discover iSNS <*iSNS address*> <*Interface name*>** command to discover all the iSCSI targets that are registered with the iSNS server on the specific interface.

You are asked to provide a username and password. Type **yes** if your target requires authentication.

Note: When CHAP authentication is enabled on a target device and targets are discovered by using iSNS, the `iSCSI > Target Discover` command may not prompt for target credentials.

```
Does your target require a username and password? (yes,no)[no]:no

Showing the discovered targets...

+-----+--------------------------|---------------------|----------------+
| No. |          Target IQN      |Target Portal Address|   Interfaces   |
+-----+--------------------------|---------------------|----------------|
|  1  | iqn.1996-03.veritas:abc  | 10.121.98.22:3260   | iscsi1, iscsi2 |
+-----+--------------------------|---------------------|----------------|
|  2  | iqn.1996-03.veritas:xyz  | 10.121.98.23:3260   | iscsi1, iscsi2 |
+-----+--------------------------|---------------------|----------------+
|  3  | iqn.1996-03.veritas:host | 10.121.98.24:3260   | iscsi1, iscsi2 |
------|--------------------------|---------------------|----------------|
```

Connecting to a target

After initiator and target connections are discovered, iSCSI initiators must be logged on to targets to establish connections and transfer data over iSCSI. Logons are persistent and connections are automatically restored if servers restart (unless the user logs off from the target).

To connect an initiator to a single target, specify the IP address of the portal and the target IQN.

To connect to a target

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.
3. Type the command **Target Connect**.
4. Enter the IQN and portal address of the discovered target. A user name is required if authentication is enabled on the target.

   Note the following about IQN, portal address, and user name:

   - The IQN can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), and periods (.)
     Example: iqn.1999-06.com.veritas:storage.lun1
   - The target portal address must be of the following format: **<IP address/hostname>[:port]**. Only IPv4 addresses are supported. The host name can be a short name or a fully qualified domain name.
     Example: 192.116.116.50 or abc:3260
   - The user name can only contain numbers (0-9), letters (A-Z and a-z), hyphens (-), underscrores (_), and periods (.). It must begin with numbers (0-9), letters (A-Z and a-z), and underscores (_) only.
     Example: john.smith
5. Run the command to connect to the target. You can connect to one discovered target at a time.

Disconnecting the sessions with a target

You can use the **iSCSI > Target Disconnect** command to disconnect sessions with the target that has the specific IQN and portal address. Once you run this command, all the sessions that are connected to this target will get disconnected.

You can disconnect sessions with one target at a time.

Note: This command takes more time to complete if workloads are running on the iSCSI interface.

To disconnect the sessions with a target

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.

3. Type the command **Target Disconnect**.
4. Enter the IQN and portal address of the target that you want to disconnect.

   Note the following about IQN and portal address:

   - The IQN can only contain numbers (0-9), letters (A-Z and a-z), colons (:), hyphens (-), and periods (.)
     Example: iqn.1999-06.com.veritas:storage.lun1
   - The target portal address must be of the following format: **<IPv4 address/hostname>[:port]**. The host name can be a short name or a fully qualified domain name.
     Example: 192.116.116.50 or abc:3260
5. Run the command to disconnect sessions with the specific target. Type **yes** when the following prompt appears:

```
Do you want to disconnect the target session?[yes, no](no):yes

[Info] The target session has been disconnected.
```

Viewing the targets

This section provides instructions on how you can view the targets. You can use the **iSCSI > Target Show** command to view all the discovered targets or the connected targets.

To view the connected targets

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.
3. Type the command **Target Show Connected** and press **Enter**.
4. The list of connected targets is displayed in the following manner:

```
Showing the connected targets...

+-----+------------+----------------------+----------------------+--------+
| No. | Session ID |      Target IQN      | Target Portal Address| Status |
+-----+------------+----------------------+----------------------|--------+
|  1  |     5      |iqn.1996-03.veritas:abc|   10.121.37.51:3260  | Online 1     |
+-----+------------+----------------------+----------------------+--------+
```

The **Status** of the session can be either **Online** or **Offline**. The **Status** can be **Offline** if a cable is pulled or if there are network connectivity issues.

To view all the available targets

1. Open a Secure Shell (SSH) session to log on to the appliance as an administrator.
2. Navigate to the **Main_Menu > Settings > iSCSI** menu.
3. Type the command **Target Show All** and press **Enter**.
4. A list of all the discovered targets is displayed in the following manner:

```
Showing all the targets...

+-----+------------------------|--------------------|-----------+
| No. |      Target IQN        |Target Portal Address|Interfaces |
+-----+------------------------|--------------------|-----------|
|  1  |iqn.1996-03.veritas:abc | 10.121.98.22:3260  | iscsi1    |
+-----+------------------------|--------------------|-----------|
|  2  |iqn.1996-03.veritas:xyz | 10.121.98.23:3260  | iscsi1    |
+-----+------------------------|--------------------|-----------+
|  3  |iqn.1996-03.veritas:host| 10.121.98.24:3260  | iscsi1    |
------|------------------------|--------------------|-----------|
```

Note: When targets are discovered by using iSNS on two iSCSI interfaces like first run the `Target Discover iSNS` command for *iscsi1* and then *iscsi2*, only the recent record is displayed by the `Target Show All` command. For example the **Interfaces** column in the `Target Show All` command may not show both the interfaces (*iscsi1*, *iscsi2*) for some targets. It actually shows the interface from the most recent command (*iscsi2* in this case) for some targets.

Chapter 5

Troubleshooting iSCSI issues and some best practices

This chapter includes the following topics:

Gathering device logs with the DataCollect command

You can use the `DataCollect` command from the `Main > Support` shell menu to gather device logs. You can share these device logs with the Veritas Support team to resolve device-related issues.

The DataCollect command collects the following logs:

- Release information
- Disk performance logs
- Command output logs
- iSCSI logs

Note: The iSCSI logs can be found in /var/log/messages and /var/log/iscsiuio.log.

- CPU information
- Memory information
- Operating system logs
- Patch logs
- Storage logs
- File system logs
- Test hardware logs
- AutoSupport logs
- Hardware information
- Sysinfo logs

To gather device logs with the DataCollect command

1. Log on to the NetBackup Appliance Shell Menu.
2. From the `Main > Support` view, type the following command to gather storage device logs.

   ```
   DataCollect
   ```

   The appliance generates the device log in the `/tmp/DataCollect.zip` file.
3. Copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.
4. You can send the `DataCollect.zip` file to the Veritas Support team to resolve your issues.

About `syslogd` messages

You may see the following messages appear on the NetBackup Appliance Shell Menu:

```
Message from syslogd@host at Sep 12 10:09:14 ...
iscsid:

Message from syslogd@host at Sep 12 10:13:27 ...
iscsid:
```

```
Message from syslogd@host at Sep 12 10:17:53 ...
iscsid:
```

These messages may appear at different times on the NetBackup Appliance Shell Menu. They may appear when you are running an iSCSI command, in the middle of a command output, or even when the console is idle. These messages are harmless and should be ignored.

About iSCSI alerts

If you have configured alerts for a specific appliance, you can also receive iSCSI alerts (as applicable). An iSCSI alert is generated in the following situations:

- An iSCSI session with the target gets disconnected (V-475-108-1000)
- An iSCSI session with the target storage server is offline (V-475-108-1001)
- An unsupported Small Form-Factor Pluggable (SFP+) module is detected in a 10 Gb Ethernet/iSCSI card (V-475-107-1000)

The following are sample iSCSI alerts:

```
An iSCSI session with the target has been disconnected.
Time of event: 2016-09-09 21:34:13 (-07:00)
UMI Event code: V-475-108-1000
Component Type: Connections
Component: <Target IQN> <Portal address> <Interface name>
Status: Disconnected
State: ERROR
Additional information about this error is available at following
link: V-475-108-1000

An iSCSI session with the target storage server is offline.
Time of event: 2016-10-13 21:34:13 (-07:00)
UMI Event code: V-475-108-1001
Component Type: Connections
Component: <Target IQN> <Portal address> <Interface name>
Status: Offline
State: ERROR
Additional information about this error is available at following
link: V-475-108-1001

The SFP+ module that is currently installed in the 10Gb Ethernet/iSCSI
card is not supported.
Time of event: 2016-10-06 18:31:42 (-07:00)
UMI Event code: V-475-107-1000
```

```
Component Type: Ethernet
Component: PCIe slot 6, port 1 SFP
Status: Unsupported
State: ERROR
Additional information about this error is available at following
link: V-475-500-1000
```

Best Practices

The following are some recommendations and best practices for iSCSI:

- Configure an IQN that is different from the default value.
  See "Setting the IQN for the initiator" on page 21.
- Configure alerts so that you can receive iSCSI-related alerts.
  See the *NetBackup Appliance Administrator's Guide* for information about configuring alerts.

Index