Dell™ Model TL2000/TL4000 1GB iSCSI to SAS bridge iSCSI initiators

Table of Contents

Install the iSCSI Initiator Software (iSCSI-attached Host Servers Only)

Your Dell™ Model TL24iSCSIxSAS 1Gb iSCSI to SAS™ bridge requires an iSCSI initiator installed in the host server. The initiator needed will depend on your host server operating system. The information in this document provides relevant information on iSCSI initiator installation and configuration. For further information and latest documentation consult www.dell.com/support

NOTE: Windows Server® 2008 contains a built-in iSCSI initiator. If your system is running Windows Server 2008, you do not need to install the iSCSI initiator Software Installation
Depending on whether you are using a Windows Server 2003 operating system or a Linux operating system, refer to the following steps for downloading and installing the iSCSI initiator.

Installing the iSCSI Initiator on a Windows Host Server

1) Refer to the Dell™ Model TL24iSCSIxSAS 1Gb iSCSI to SAS™ bridge Support Matrix located at: //www.support.dell.com for the latest version and download location of the Microsoft iSCSI Software Initiator software
2) From the host server, download the iSCSI Initiator software
3) Once the installation begins and the Microsoft iSCSI Initiator Installation setup panel appears, select Initiator Service and Software Initiator.
4) DO NOT select Microsoft MPIO Multitpathing Support for iSCSI.

NOTICE: Make sure the Microsoft MPIO Multitpathing Support for iSCSI option is NOT selected. Using this option will cause the iSCSI initiator setup to function improperly.

5) Accept the license agreement and finish the install.

NOTE: If you are prompted to do so, reboot your system.

Installing the iSCSI Initiator on a Linux Host Server

You can install the iSCSI initiator software on Red Hat® Enterprise Linux® 4 systems either during or after operating system installation.

Installing the iSCSI initiator during RHEL 4 installation:

1) When the Package Installation Defaults screen is displayed, select the Customize the set of Packages to be installed option. Click Next to go to the Package Group Selection screen.
2) In the Servers list, select the Network Servers package and click Details to display a list of Network Server applications.
3) Select the iscsi-initiator-utils - iSCSI daemon and utility programs option.
4) Click OK, then Next to continue with the installation.

Installing the iSCSI initiator after RHEL 4 installation:

1) From the desktop, click Applications–> System Settings–>Add Remove Applications. The Package Group Selection screen is displayed.
2) In the Servers list, select the Network Servers package and click Details to display a list of Network Server applications.
3) Select the iscsi-initiator-utils - iSCSI daemon and utility programs option.
4) Click Close, then Update.

NOTE: Depending upon your installation method, the system will ask for the required source to install the package.

Installing the iSCSI Initiator on a RHEL 5 System

You can install the iSCSI initiator software on Red Hat Enterprise Linux 5 systems either during or after operating system installation. With this version of the Linux software, you can also elect to install the iSCSI initiator after the operating system installation via the command line.

Installing the iSCSI initiator during RHEL 5 installation:

1) When the Package Installation Defaults screen is displayed, select the Customize now option.
2) Click Next to go to the Package Group Selection screen.
3) Select Base System, then select the Base option.
4) Click Optional Packages.
5) Select the iscsi-initiator-utils option.
6) Click OK, then Next to continue with the installation.

Installing the iSCSI initiator after RHEL 5 installation:

1) From the desktop, select Applications Add/Remove Software. The Package Manager screen is displayed.
2) In the Package Manager screen, select the Search tab.
3) Search for `iscsi-initiator-utils`.
4) When it is displayed, select the iscsi-initiator-utils option.
5) Click Apply.

NOTE: Depending upon your installation method, the system will ask for the required source to install the package.
NOTE: This method might not work if network access is not available to a Red Hat Network repository.

Installing the iSCSI initiator after RHEL 5 installation via the command line:

1) Insert the RHEL 5 installation CD 1 or DVD. If your media is not automounted, you must manual mount it. The iscsi-initiatorutils.rpm file is located in the Server or Client subdirectory.
2) Run the following command: `rpm -i /path/to/media/Server/iscsi-initiatorutils.rpm`

Installing the iSCSI Initiator on a SLES 9 System

You can install the iSCSI initiator software on SUSE® Linux Enterprise Servers (SLES) 9 SP3 systems either during or after operating system installation.

Installing the iSCSI initiator during SLES 9 installation:

1) At the YaST Installation Settings screen, click Change.
2) Click Software, then select Detailed Selection to see a complete list of packages.
3) Select Various Linux Tools, then select linux-iscsi.
4) Click Accept. If a dependencies window is displayed, click Continue and proceed with the installation.

Installing the iSCSI initiator after SLES 9 installation:

1) From the Start menu, select System YaST.
2) Select Software, then Install and Remove Software.
3) In the Search box, enter `linux-iscsi`.

4) When the linux-iscsi module is displayed, select it.
5) Click on Check Dependencies to determine if any dependencies exist.
6) f no dependencies are found, click Accept.

Installing the iSCSI Initiator on a SLES 10 SP1 System

You can install the iSCSI initiator software on SUSE Linux Enterprise Server Version 10 systems either during or after operating system installation.

Install the iSCSI initiator during SLES 10 SP1 installation:

1) At the YaST Installation Settings screen, click Change.
2) Click Software, then select Search.
3) In the Search box, enter `iscsi`.
4) When the open-iscsi and yast2-iscsi-client modules are displayed, select them.
5) Click Accept.
6) If a dialog box regarding dependencies appears, click Continue and proceed with installation.

Installing the iSCSI initiator after SLES 10 SP1 installation:

1) Select Desktop YaST Software Software Management.
2) Select Search.
3) In the Search box, enter `iscsi`. Software Installation 23
4) When the open-iscsi and yast2-iscsi-client modules are displayed, select them.
5) Click Accept.

Perform Target Discovery from the iSCSI Initiator

This step identifies the iSCSI ports on the TL2000/TL4000 1GB iSCSI to SAS bridge. Select the set of steps that correspond to your operating system (Windows or Linux).

Using Windows Server 2003 or Windows Server 2008 GUI version

1) Click Start–> Programs–> Microsoft iSCSI Initiator or Start–> All Programs–> Administrative Tools–> iSCSI Initiator.
2) Click the Discovery tab.
3) Under Target Portals, click Add and enter the IP address or DNS name of the iSCSI to SAS port on the bridge.
4) If the iSCSI to SAS bridge uses a custom TCP port, change the Port number. The default is 3260.
5) Click Advanced and set the following values on the General tab:
    a) Local Adapter: Must be set to Microsoft iSCSI Initiator.
    b) Source IP: The source IP address of the host you want to connect with.
    c) Data Digest and Header Digest: Optionally, you can specify that a digest of data or header information be compiled during transmission to assist in troubleshooting.
    d) CHAP logon information: Leave this option unselected and do not enter CHAP information at this point, unless you are adding the iSCSI to SAS Bridge to a SAN that has target CHAP already configured. See configure CHAP authentication on host server.

    NOTE: IPSec is not supported.

    e) Click OK to exit the advanced menu, and OK again to exit the Add Target Portals screen.
6) To exit the Discovery tab, click OK.
7) Repeat step 3 thorough step 6 (above) for the second network port in your iSCSI to SAS bridge

Using Windows Server 2008 Core Version

1) Set the iSCSI initiator service to start automatically: `\\<server_name> config msiscsi start= auto`
2) Start the iSCSI service: `start msiscsi`
3) Add a target portal: `iscsicli QAddTargetPortal <IP_address_of_iSCSI_port_on_storagearray>`

Using Linux Server

Configuration of the iSCSI initiator for Red Hat® Enterprise Linux® version 4 and SUSE® Linux Enterprise Server 9 distributions is performed by modifying the /etc/iscsi.conf file, which is installed by default when you installed the iSCSI initiator. The /etc/iscsi.conf file needs to be changed before using the initiator:

1) Edit the /etc/iscsi.conf file and replace the IP address entries shown for `DiscoveryAddress=` with the IP addresses assigned to the iSCSI ports on your iSCSI to SAS bridge:
2) Edit (or add) the following entries to the /etc/iscsi.conf file:

```
HeaderDigest=never
DataDigest=never
LoginTimeout=15
IdleTimeout=15
PingTimeout=5
ConnFailTimeout=144
AbortTimeout=10
ResetTimeout=30
Continuous=no
InitialR2T=no
ImmediateData=yes
MaxRecvDataSegmentLength=65536
FirstBurstLength=262144
MaxBurstLength=16776192
```

3) Restart the iSCSI daemon by executing the following command from the console: `/etc/init.d/iscsi restart`
4) Verify that the server can connect to the iSCSI to SAS bridge by executing this command from a console: `iscsi –ls.` If successful, an iSCSI session has been established to each iSCSI port on the iSCSI to SAS bridge.

Using RHEL 5 or SLES 10 SP1

Configuration of the iSCSI initiator for RHEL version 5 and SLES 10 SP1 distributions is done by modifying the /etc/iscsi/iscsid.conf file.

1) Edit the following entries in the /etc/iscsi/iscsid.conf file:
   a) Edit (or verify) that the `node.startup = manual` line is disabled.
   b) Edit (or verify) that the `node.startup = automatic` line is enabled. This will enable automatic startup of the service at boot time.
   c) Verify that the following time-out value is set to 144: `node.session.timeo.replacement_timeout = 144`
   d) Save and close the /etc/iscsi/iscsid.conf file.
2) From the console, restart the iSCSI service with the following command: `service iscsi start`
3) Verify that the iSCSI service is running during boot using the following command from the console: `chkconfig iscsi on`
4) To display the available iscsi targets at the specified IP address, use the following command: `iscsiadm –m discovery –t st -p <IP_address_of_iSCSI_port>`
5) After target discovery, use the following command to manually login: `iscsiadm -m node –l.` This logon will be performed automatically at startup if automatic startup is enabled.
6) Manually log out of the session using the following command: `iscsiadm -m node -T <initiator_username> -p <target_ip> -u`

Configure CHAP Authentication on the Host Server (optional)

Select the set of steps in one of the following sections (Windows or Linux) that corresponds to your operating system.

Using Windows Server 2003 or Windows Server 2008 GUI version

1) Click Start –>Programs–>Microsoft iSCSI Initiator or Start –>All Programs–>Administrative Tools–> iSCSI Initiator.
2) If you are using mutual CHAP authentication:
   a) Click the General tab
   b) Select Secret
   c) Enter a secure secret, enter the mutual CHAP secret you entered for the iSCSI to SAS bridge
3) Click the Discovery tab.
4) Under Target Portals, select the IP address of the iSCSI port on iSCSI bridge and click Remove. The iSCSI port you configured on the iSCSI to SAS bridge during target discovery should disappear. You will reset this IP address under CHAP authentication in the steps that immediately follow.
5) Under Target Portals, click Add and re-enter the IP address or DNS name of the iSCSI port on the iSCSI bridge (removed above).
6) Click Advanced and set the following values on the General tab:
   d) Local Adapter: Should always be set to Microsoft iSCSI Initiator.
   e) Source IP: The source IP address of the host you want to connect with.
   f) Data Digest and Header Digest: Optionally, you can specify that a digest of data or header information be compiled during transmission to assist in troubleshooting.
   g) CHAP logon information: Enter the target CHAP authentication username and secret you entered (for the host server) on the iSCSI to SAS bridge.
   h) Perform mutual authentication: If mutual CHAP authentication is configured, select this option.

   NOTE: IPSec is not supported.
7) Click OK.

Using Windows Server 2008 Core Version

1) Set the iSCSI initiator services to start automatically (if not already set): sc \\<server_name> config msiscsi start= auto
2) Start the iSCSI service (if necessary): sc start msiscsi
3) If you are not using mutual CHAP authentication, skip to step 4.
4) Enter the mutual CHAP secret you entered for the iSCSI to SAS bridge: iscsicli CHAPSecret <secret>
5) Remove the target portal that you configured on the iSCSI to SAS bridge during target discovery: `iscsicli RemoveTargetPortal <IP_address> <TCP_listening_port>`
6) You will reset this IP address under CHAP authentication in the following steps.

   Add the target portal with CHAP defined:

   ```
   iscsicli QAddTargetPortal
   <IP_address_of_iSCSI_port_on_storage_array>
   [CHAP_username][CHAP_password]
   ```

   where

   `[CHAP_username]` is the initiator name

   `[CHAP_password]` is the target CHAP secret

Using Linux Server

1) Edit the /etc/iscsi.conf file to add the entries below for each iSCSI target:

For example, your edited /etc/iscsi.conf file might look like this:

```
DiscoveryAddress=172.168.10.6
OutgoingUsername=iqn.1987-05.com.cisco:01.742b2d31b3e
OutgoingPassword=0123456789abcdef
```

Note: If you are configuring Mutual CHAP authentication in Linux, you must also add an `IncomingUsername=` and `IncomingPassword=` entry after each `OutgoingPassword=` entry.
The IncomingUsername is the iSCSI target name, which can be viewed in the iSCSI bridge management interface

For example, your edited /etc/iscsi.conf file might look like this:

```
DiscoveryAddress=172.168.10.6
OutgoingUsername=iqn.1987-05.com.cisco:01.742b2d31b3e
OutgoingPassword=0123456789abcdef
IncomingUsername=iqn.1984-05.com.dell:powervault.6001372000f5f0e600000000463b9292
IncomingPassword=abcdef0123456789
```

If you are using RHEL 5 or SLES 10 SP1

1) To enable CHAP, add the following line to your /etc/iscsi/iscsid.conf file.
```
node.session.auth.authmethod = CHAP
```
2) To set a username and password for CHAP authentication of the initiator by the target(s), edit the following lines as shown:
```
node.session.auth.username = <iscsi_initiator_username>
node.session.auth.password = <CHAP_initiator_password>
```
3) If you are using Mutual CHAP authentication, you can set the username and password for CHAP authentication of the target(s) by the initiator by editing the following lines:
```
node.session.auth.username_in= <iscsi_target_username>
node.session.auth.password_in = <CHAP_target_password>
```
4) To set up discovery session CHAP authentication, first uncomment the following line:
```
discovery.sendtargets.auth.authmethod = CHAP
```
5) Set a username and password for a discovery session CHAP authentication of the initiator by the target(s) by editing the following lines:
```
discovery.sendtargets.auth.username = <iscsi_initiator_username>
discovery.sendtargets.auth.password = <CHAP_initiator_password>
```
6) To set the username and password for discovery session CHAP authentication of the target(s) by the initiator for Mutual CHAP, edit the following lines:
```
discovery.sendtargets.auth.username = <iscsi_target_username>
discovery.sendtargets.auth.password_in = <CHAP_target_password>
```
7) As a result of steps 1 through 6, the final configuration contained in the /etc/iscsi/iscsid.conf file might look like this:
```
node.session.auth.authmethod = CHAP
node.session.auth.username = iqn.2005-03.com.redhat01.78b1b8cad821
node.session.auth.password = password_1
node.session.auth.username_in= iqn.1984-
05.com.dell:powervault.123456
node.session.auth.password_in = test1234567890
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = iqn.2005-
03.com.redhat01.78b1b8cad821
discovery.sendtargets.auth.password = password_1
discovery.sendtargets.auth.username = iqn.1984-
05.com.dell:powervault.123456
discovery.sendtargets.auth.password_in = test1234567890
```

If you are using SLES10 SP1 via the GUI

1) Select Desktop–> YaST–>iSCSI Initiator.

2) Click Service Start; then select When Booting.
3) Select Discovered Targets; then select Discovery.
4) Enter the IP address of the port.
5) Click Next.
6) Select any target that is not logged in and click Log in.
7) Choose one:
8) If you are not using CHAP authentication, select No Authentication. Proceed to step 11.
9) If you are using CHAP authentication, enter the CHAP username and password. To enable
10) Mutual CHAP, select and enter the Mutual CHAP username and password.
11) Repeat step 7 for each target until at least one connection is logged in for each controller.
12) Go to Connected Targets.
13) Verify that the targets are connected and show a status of true.

Connect to the TL2000/TL4000 from the Host Server

If you are using Windows Server 2003 or Windows Server 2008 GUI

1) Click Start–> Programs–> Microsoft iSCSI Initiator or Start–> All Programs–>Administrative Tools–> iSCSI Initiator.
2) Click the Targets tab. If previous target discovery was successful, the iqn of the iSCSI to SAS bridge should be displayed under Targets.
3) Click Log On.
4) Select automatically restore this connection when the system boots.
5) Select Enable multi-path.
6) Click Advanced and configure the following settings under the General tab:
   a) Local Adapter: Must be set to Microsoft iSCSI Initiator.
   b) Source IP: The source IP address of the host server you want to connect from.
   c) Target Portal: Select the iSCSI port on the iSCSI to SAS bridge controller that you want to connect to.
   d) Data Digest and Header Digest: Optionally, you can specify that a digest of data or header information be compiled during transmission to assist in troubleshooting.
   e) CHAP logon information: If CHAP authentication is required, select this option and enter the Target secret.
   f) Perform mutual authentication: If mutual CHAP authentication is configured, select this option.

NOTE: IPSec is not supported.

7) Click OK.

NOTE: To enable the higher throughput of multipathing I/O, the host server must connect to both iSCSI ports on the iSCSI to SAS bridge, ideally from separate host-side NICs.

8) Repeat step 3 through step 7 for 2nd iSCSI port on the bridge
   The Status field on the Targets tab should now display as Connected.
9) Click OK to close the Microsoft iSCSI initiator.

If you are using Windows Server 2008 Core Version

1) Set the iSCSI initiator services to start automatically (if not already set): `sc \\<server_name> config msiscsi start= auto`
2) Start the iSCSI service (if necessary): `sc start msiscsi`
3) Log on to the target:

```
iscsicli PersistentLoginTarget <Target_Name> <Report_To_PNP>
<Target_Portal_Address> <TCP_Port_Number_Of_Target_Portal> * * *
<Login_Flags> * * * * * <Username> <Password> <Authtype> *
<Mapping_Count>
```

where

`<Target_Name>` is the target name as displayed in the target list. Use the `iscsicli`

`ListTargets` command to display the target list.
`<Report_To_PNP>` is T, which exposes the LUN to the operating system as a storage device.
`<Target_Portal_Address>` is the IP address of the iSCSI port on the controller being logged into.
`<TCP_Port_Number_Of_Target_Portal>` is `3260`.
`<Login_Flags>` is `0x2` to enable multipathing for the target on the initiator. This value allows more than one session to be logged in to a target at one time.
`<Username>` is the initiator name.
`<Password>` is the target CHAP secret.
`<Authtype>` is either `0` for no authentication, `1` for Target CHAP, or `2` for Mutual CHAP.

NOTE: <*Username*>, <*Password*> and <*Authtype*> are optional parameters. They can be replaced with an asterisk (*) if CHAP is not used.
`<Mapping_Count>` is `0`, indicating that no mappings are specified and no further parameters are required.
`* * *` An asterisk (*) represents the default value of a parameter.
For example, your logon command might look like this:

```
iscsicli PersistentLoginTargetiqn.1984-
05.com.dell:powervault.6001372000ffe333000000004672edf2
3260 T 192.168.130.101 * * * 0x2 * * * * * * * * * 0
```

To view active sessions to the target, use the following command: `iscsicli SessionList`

`PersistentLoginTarget` does not initiate a login to the target until after the system is rebooted. To establish immediate login to the target, substitute `LoginTarget` for `PersistentLoginTarget`.

NOTE: Refer to the *Microsoft iSCSI Software Initiator 2.x User's Guide* for more information about the commands used in the previous steps. For more information about Windows Server 2008 Server Core, refer to the Microsoft Developers Network (MSDN). Both resources are available at www.microsoft.com.

If you are using a Linux Server

If you configured CHAP authentication in the previous steps, you must restart iSCSI from the Linux command line as shown below. If you did not configure CHAP authentication, you do not need to restart iSCSI.

```
/etc/init.d/iscsi restart
```

Verify that the host server is able to connect to the iSCSI to SAS bridge by running the iscsi -ls command as you did in target discovery. If the connection is successful, an iSCSI session will be established to each iSCSI port on the iSCSI to SAS bridge.
Sample output from the command should look similar to this:

```
*******************************************************************************
SFNet iSCSI Driver Version ...4:0.1.11-3(02-May-2006)
*******************************************************************************
TARGET NAME : iqn.1984-05.com.dell:powervault.6001372000f5f0e600000000463b9292
TARGET ALIAS :
HOST ID : 2
BUS ID : 0
TARGET ID : 0
TARGET ADDRESS : 192.168.0.110:3260,1
SESSION STATUS : ESTABLISHED AT Wed May 9 18:20:27 CDT 2007
SESSION ID : ISID 00023d000001 TSIH 5
*******************************************************************************
TARGET NAME : iqn.1984-05.com.dell:powervault.6001372000f5f0e600000000463b9292
TARGET ALIAS :
HOST ID : 3
BUS ID : 0
TARGET ID : 0
TARGET ADDRESS : 192.168.0.111:3260,1
```

Setting Up Your iSCSI ISCSI to SAS bridge 57

```
SESSION STATUS : ESTABLISHED AT Wed May 9 18:20:28 CDT 2007
SESSION ID : ISID 00023d000002 TSIH 4
```

****

Guidelines for Configuring Your Network for iSCSI

This section gives general guidelines for setting up your network environment and IP addresses for use with the iSCSI ports on your host server and iSCSI to SAS bridge. Your specific network environment may require different or additional steps than shown here, so make sure you consult with your system administrator before performing this setup.

Windows Host Setup

If you are using a Windows host network, the following section provides a framework for preparing your network for iSCSI.

To set up a Windows host network, you must configure the IP address and netmask of each iSCSI port connected to the iSCSI to SAS Bridge. The specific steps depend on whether you are using a Dynamic Host Configuration Protocol (DHCP) server, static IP addressing, Domain Name System (DNS) server, or Windows Internet Name Service (WINS) server.

NOTE: The server IP addresses must be configured for network communication to the same IP subnet as the iSCSI to SAS bridge management and iSCSI ports.

If using a DHCP server

1) On the Control Panel, select Network connections or Network and Sharing Center. Then click Manage network connections.
2) Right-click the network connection you want to configure and select Properties
3) On the General tab (for a local area connection) or the Networking tab (for all other connections), select Internet Protocol (TCP/IP), and then click Properties.
4) Select Obtain an IP address automatically, then OK.

If using Static IP addressing

1) On the Control Panel, select Network connections or Network and Sharing Center. Then click Manage network connections.
2) Right-click the network connection you want to configure and select Properties.
3) On the General tab (for a local area connection) or the Networking tab (for all other connections), select Internet Protocol (TCP/IP), and then click Properties.

If using a DNS server

1) On the Control Panel, select Network connections or Network and Sharing Center. Then click Manage network connections.
2) Right-click the network connection you want to configure and select Properties.
3) On the General tab (for a local area connection) or the Networking tab (for all other connections), select Internet Protocol (TCP/IP), and then click Properties.
4) Select Obtain DNS server address automatically or enter the preferred and alternate DNS server IP addresses and click OK.

If using a WINS server

NOTE: If you are using a DHCP server to allocate WINS server IP addresses, you do not need to add WINS server addresses.

1) On the Control Panel, select Network connections.
2) Right-click the network connection you want to configure and select Properties.
3) On the General tab (for a local area connection) or the Networking tab (for all other connections), select Internet Protocol (TCP/IP), and then click Properties.
4) Select Advanced, then the WINS tab, and click Add.
5) In the TCP/IP WINS server window, type the IP address of the WINS server and click Add.

6) To enable use of the Lmhosts file to resolve remote NetBIOS names, select Enable LMHOSTS lookup.
7) To specify the location of the file that you want to import into the Lmhosts file, select Import LMHOSTS and then select the file in the Open dialog box
8) Enable or disable NetBIOS over TCP/IP.

If using Windows 2008 Core Version

On a server running Windows 2008 Core version, use the netsh interface command to configure the iSCSI ports on the host server.

Linux Host Setup

If you are using a Linux host network, the following section provides a framework for preparing your network for iSCSI.

To set up a Linux host network, you must configure the IP address and netmask of each iSCSI port connected to the .The specific steps depend on whether you are configuring TCP/IP using Dynamic Host Configuration Protocol (DHCP) or configuring TCP/IP using a static IP address.

Network Configuration Guidelines

NOTE: The server IP addresses must be configured for network communication to the same IP subnet as the iSCSI to SAS bridge management and iSCSI ports.

Configuring TCP/IP on Linux using DHCP (root users only)

1) Edit the /etc/sysconfig/network file as follows:
```
NETWORKING=yes
HOSTNAME=mymachine.mycompany.com
```
2) Edit the configuration file for the connection you want to configure, either /etc/sysconfig/networkscripts/ifcfg-ethX (for RHEL) or /etc/sysconfig/network/ifcfg-eth-id-XX:XX:XX:XX:XX (for SUSE). `BOOTPROTO=dhcp`
Also, verify that an IP address and netmask are not defined.
3) Restart network services using the following command:
```
/etc/init.d/network restart
```

Configuring TCP/IP on Linux using a Static IP address (root users only)

1) Edit the /etc/sysconfig/network file as follows:
```
NETWORKING=yes
HOSTNAME=mymachine.mycompany.com
GATEWAY=255.255.255.0
```
2) Edit the configuration file for the connection you want to configure, either /etc/sysconfig/networkscripts/ifcfg-ethX (for RHEL) or /etc/sysconfig/network/ifcfg-eth-id-XX:XX:XX:XX:XX (for SUSE).
```
BOOTPROTO=static
BROADCAST=192.168.1.255
IPADDR=192.168.1.100
NETMASK=255.255.255.0
NETWORK=192.168.1.0
ONBOOT=yes
TYPE=Ethernet
HWADDR=XX:XX:XX:XX:XX:XX
GATEWAY=192.168.1.1
```
3) Restart network services using the following command:
```
/etc/init.d/network restart
```

Avoiding duplicate iSCSI devices discovered by RH5

To kill the unwanted sessions on the duplicate devices, do the following:

1) From the command line, type in ‘iscsi-ls’

This will list all the iSCSI devices that have sessions opened. Look for the duplicate Drive and Library entries. (i.e., if you have four entries, two might be the tape drive (spi.1.0.0), and two might be for the library (spi.1.0.1)

Each entry will have a unique Host ID associated with it (i.e., Host ID 65 might be for the first spi.1.0.0, while Host ID 66 might be for the second spi.1.0.0 entry)

2) Select one of the Host ID’s that is associated for the drive, and one of the Host ID’s that is associated for the libraries. (i.e., if the drive has Host ID 65 and 66, note ID 66; if the library has Host ID’s 67 and 68, note ID 68

```
From the Linux command line, type ‘iscsi-kill-session –i 66
From the Linux command line, type ‘iscsi-kill-session –i 68
```

If you run the ‘iscsi-ls’ again, you should only see a single instance for the drive, and a single instance for the library.

Note: every time you restart the iscsi services, all the sessions will be opened back up again. Also, the session ID’s change, so it will be necessary to go back thru the steps above to kill the new iscsi sessions.

Avoiding duplicate iSCSI devices discovered by RH4

To avoid logging in to multiple devices that were identified in a iSCSI Discovery (i.e., when starting the iSCSI services), make the following changes to your RedHat 4 iscsi.conf file located in the /etc directory. Make sure you restart the service after making these changes.

```
# --------------------------
# Discovery Address Category
# --------------------------
      DiscoveryAddress=192.168.1.133:3260
      DiscoveryAddress=192.168.2.133:3260
```

Specify the IP address(s) and corresponding ports of the target devices that you want to discover.

Note: Even though you only specify these target devices, other devices might be discovered when starting the service. An exclusion of everything that you do not want will be done next.

```
ENABLE/DISABLE TARGETS
# ----------------------
      TargetName=iqn.1988-11.com.dell.2005c5:spi.0.0.0
      Enabled=no
      TargetName=iqn.1988-11.com.dell.2005c5:spi.0.0.1
      Enabled=no
```

The iscsi.conf statements above will disable the individual targets that you do not want to log in to. In the example above, the target that contains spi.0.0.0 is an LT04 tape drive, while the target that contains 0.0.1 is the device that represents the Medium Changer.

To verify that the correct target devices are removed (and the correct ones remain), ensure your iscsi services are running, and enter ‘iscsi-ls’. It will provide you a listing of all the devices that were discovered and enabled.

Viewing the status of your iSCSI connections

In ISCSI Web Manager interface, click the iSCSI connections, the Host Ports will show the status of each iSCSI port you attempted to connect and the configuration state of all IP addresses. If connections are not present, Check the following:

- Are all cables securely attached to each port on the host server and iSCSI to SAS bridge?
- Is TCP/IP correctly configured on all target host ports?
- Is CHAP set up correctly on both the host server and the iSCSI to SAS bridge?

- Review optimal network setup and configuration settings; see Guidelines for Configuring Your Network for iSCSI.

Performing Hardware Maintenance with your iSCSI solution

The iSCSI initiators required being log out and targets removed when making hardware configurations changes. Ensure the following:

1) Backup applications are down (close the application or stop the services)
2) Open the iSCSI initiator
3) Log out of the current targets
4) Delete the target IP address targets
5) Perform your HW update
6) Re-configure your iSCSI initiator
7) Re-configure you ISV

Note: To delete the targets in Linux use the command below:

```
iscsiadm --mode node –T iqn.1988-11.com.dell.2000eb:eui.5000e11116c35003.0 --op=delete
iscsiadm --mode node –T iqn.1988-11.com.dell.2000eb:eui.5000e11116c35003.1 --op=delete
```

Reference information

Terminology

CHAP (Challenge Handshake Authentication Protocol). An optional security protocol used to control access to an iSCSI storage system by restricting use of the iSCSI data ports on both the host server and iSCSI to SAS bridge. For more information on the types of CHAP authentication supported, see Understanding CHAP Authentication.
Host server port iSCSI port on the host server used to connect it to bridge.
iSCSI initiator The iSCSI-specific software installed on the host server that controls communications between the host server and the iSCSI to SAS bridge.

NOTE: A NOTE indicates important information that helps you make better use of your computer.
NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

Understanding CHAP Authentication

Before proceeding to either Step 5: Configure CHAP Authentication on the ISCSI to SAS bridge (optional) or
Step 6: Configure CHAP Authentication on the Host Server (optional), it would be useful to gain an overview of how CHAP authentication works.

What is CHAP?

Challenge Handshake Authentication Protocol (CHAP) is an optional iSCSI authentication method where the iSCSI to SAS bridge (target) authenticates iSCSI initiators on the host server. Two types of CHAP are supported: target CHAP and mutual CHAP.

Target CHAP

In target CHAP, the iSCSI to SAS bridge authenticates all requests for access issued by the iSCSI initiator(s) on the host server via a CHAP secret. To set up target CHAP authentication, you enter a CHAP secret on the iSCSI to SAS bridge, then configure each iSCSI initiator on the host server to send that secret each time it attempts to access the iSCSI to SAS bridge.

Mutual CHAP

In addition to setting up target CHAP, you can set up mutual CHAP in which both the iSCSI to SAS bridge and the iSCSI initiator authenticate each other. To set up mutual CHAP, you configure the iSCSI initiator with a CHAP secret that the iSCSI to SAS bridge must send to the host sever in order to establish a connection.
In this two-way authentication process, both the host server and the iSCSI to SAS bridge are sending information that the other must validate before a connection is allowed.
CHAP is an optional feature and is not required to use iSCSI. However, if you do not configure CHAP authentication, any host server connected to the same IP network as the iSCSI to SAS bridge can read from and write to the iSCSI to SAS bridge.

Using iSNS

iSNS (Internet Storage Naming Service) Server, supported only on Windows iSCSI environments, eliminates the need to manually configure each individual iSCSI to SAS bridge with a specific list of initiators and target IP addresses. Instead, iSNS automatically discovers, manages, and configures all iSCSI devices in your environment.
For more information on iSNS, including installation and configuration, see www.microsoft.com

August 2008