

This document describes how to configure iSCSI initiator ports and how to set up iSCSI security on a server connected to the iSCSI data ports on CX4 series, CX3 UltraScale™ series, CX series, AX4–5 series, and AX150 series storage systems.

We recommend that you use this guide in conjunction with one of the following guides, which are available on the [Powerlink](#) website:

- ◆ the storage-system setup guide (AX4–5 series with Navisphere Express, CX4 series, CX3 series, or CX series storage systems)
- ◆ the storage-system getting started guide (AX150 series storage systems with Navisphere Express)
- ◆ the installation roadmap (P/N 069001166) (AX4–5 series or AX150 series with Navisphere Manager, CX4 series, CX3 series, or CX series storage systems)

IMPORTANT

For more information on supported operating system revisions, driver types, or features, refer to the E-Lab™ Interoperability Navigator on the [Powerlink](#) website for CX4 series, CX3 series, or CX series storage systems, and the *Support Matrix* link on the **Install** page of the storage-system support website for AX4-5 series or AX series storage systems.

Topics include:

- ◆ Before you start 3
- ◆ iSCSI server setup process overview 6
- ◆ Installing NIC or HBA iSCSI initiator software 7
- ◆ Assigning an IP address to a NIC or iSCSI HBA 8
- ◆ Configuring NIC or iSCSI HBA initiators 10
- ◆ Preparing for CHAP security 18

- ◆ Configuring CHAP on the iSCSI initiators..... 19
- ◆ Modifying CHAP credentials on the server 32

Before you start

Before you use this guide to set up iSCSI initiator ports on the server or to set up iSCSI security (Challenge Handshake Authentication Protocol – CHAP), you must:

- ◆ configure the storage-system iSCSI ports as described in the storage-system setup guide, the storage-system getting started guide, or the installation roadmap (storage systems with Navisphere Manager only).
- ◆ complete the worksheets in the storage system configuration planning guide that either shipped with your storage system or that you generated from the customized storage-system support website.

For AX4-5 series or AX150 series, you can generate a planning guide using the **Plan** link on the **Install** page of the storage-system support website.

For CX4 series, CX3 series or CX series, you can generate a planning guide using the **Plan** link on the storage-system support website.

For more information on CHAP security, refer to the *CHAP security overview*, page 4. Otherwise, refer to the *iSCSI server setup process overview*, page 6.

Terms used in this guide

The table below lists the storage system terms used in this guide.

Table 1 Storage system models

Storage system term	Refers to
CX4 series	CX4-120, CX4-240, CX4-480, and CX4-960 storage systems
CX3 series	CX3 model 10 systems, CX3 model 20 systems, CX3 model 40 systems, and CX3 model 80 storage systems
CX series	CX200, CX300 series, CX400, CX500 series, CX600, and CX700 storage systems
AX4-5 series	AX4-5SC, AX4-5SCi, AX4-5, AX4-5i storage systems

Storage system term	Refers to
AX series	AX150 series systems, which include the AX150SC, AX150SCi, AX150, and AX150i storage systems

CHAP security overview

Challenge Handshake Authentication Protocol (CHAP) is a method of authenticating iSCSI users. The iSCSI storage system can use CHAP to authenticate initiators and initiators can likewise authenticate targets such as the storage system.



CAUTION

If you do *not* configure CHAP security for the storage system, any host connected to the same IP network as the storage-system iSCSI ports can read from and write to the storage system. If the storage system is on a *private* network, you can choose not to use CHAP security. If the storage system is on a *public* network, we strongly recommend that you use CHAP security.

If you want to use CHAP security, you must set up and enable it on both the server and storage system before preparing LUNs or virtual disks to receive data. If you prepare disks to receive data before you set up and enable CHAP security, you lose access to the LUNs or virtual disks. While you are setting up and enabling CHAP, you may temporarily lose connectivity between the server and the storage system.

CHAP has the following two variants:

- ◆ **Initiator CHAP** - Sets up accounts that iSCSI initiators use to connect to targets. The target authenticates the initiator. Initiator CHAP is the primary CHAP authentication method.

Navisphere Express provides **Basic** and **Advanced** initiator CHAP options. Basic CHAP specifies one *secret* (password) for all initiators that log in to a given target. The **Advanced** option allows you to specify a different secret for each initiator, and also allows you to set up mutual CHAP.

- ♦ **Mutual CHAP** - Applied *in addition* to initiator CHAP, mutual CHAP sets up an account that a target uses to connect to an initiator. The initiator authenticates the target.

iSCSI server setup process overview

The following overview describes the steps required for configuring iSCSI initiator ports and setting up iSCSI security.

Configuring iSCSI initiator ports

- ❑ Install the network interface card (NIC) or host bus adapter (HBA) iSCSI initiator software on each server with NICs or iSCSI HBAs that you will connect to the storage system as described in *Installing NIC or HBA iSCSI initiator software*, page 7.
- ❑ Assign an IP address for the NICs or iSCSI HBAs as described in *Assigning an IP address to a NIC or iSCSI HBA*, page 8.
- ❑ Configure initiator network parameters for the NIC or HBA iSCSI initiators as described in *Configuring NIC or iSCSI HBA initiators*, page 10.

Setting up iSCSI security

- ❑ Prepare for setting up CHAP on the server as described in *Preparing for CHAP security*, page 18.
- ❑ Configure initiator and mutual (optional) CHAP on each NIC or iSCSI HBA initiator as described in *Configuring CHAP on the iSCSI initiators*, page 19.

Installing NIC or HBA iSCSI initiator software

You must install NIC or HBA iSCSI initiator software on each server with NICs or iSCSI HBAs that you will connect to the storage system.

For iSCSI HBAs, install the QLogic SANsurfer software as described in *Downloading and installing the QLogic SANsurfer software for iSCSI HBAs*, page 7.

The iSCSI initiator software for NICs is the **iscsi_sfnet driver** or the **open-iscsi driver** that is bundled with the versions of Linux required for iSCSI configurations.

Downloading and installing the QLogic SANsurfer software for iSCSI HBAs

1. Download the QLogic SANsurfer software on the server:
 - a. Open a web browser and connect to the QLogic website:
http://support.qlogic.com/support/oem_emc.asp
 - b. Go to the **Downloads** page.
 - c. Select the HBA.

For information on supported software for an AX4-5 series, AX150 series, or AX100 series, refer to *Supported Configurations* in “Technical descriptions” on the storage-system support website.

For information on supported software for a CX4 series, CX3 series, or CX series storage system, refer to the E-Lab Interoperability Navigator on the Powerlink website:
<http://Powerlink.EMC.com>

- d. Select and download the software and related documentation.
2. Install the software as described in the QLogic documentation.

Assigning an IP address to a NIC or iSCSI HBA

Assign an IP address to *each* NIC or iSCSI HBA in the server that will be connected to the storage system.

For the NIC or iSCSI HBA IP addresses, refer to the iSCSI target and initiator port network information worksheet, which you should have completed when you planned your configuration using the *Administration Worksheet* and the configuration and planning guide.

Assigning an IP address to a NIC in a Linux server

Configure the IP information for the NIC. Some NIC vendors recommend that each NIC is on a different subnet. Open the appropriate Linux System Tool provided with the operating system, or update the system's configuration manually.

For example, in Red Hat, you can use the **Network Device Control Utility** to configure the NIC, and in SuSE, you can use **YaST** to configure the NIC.

There are several ways to assign an IP address to a NIC, depending on the version of Linux the server is running.

If the NIC is a replacement for a previously installed NIC, assign it the same IP address as the NIC it replaced, so that it automatically has the same iSCSI initiator settings and optional CHAP security settings as the NIC it replaced.

Assigning an IP address to an iSCSI HBA in a Linux server

1. Open QLogic SANsurfer as described in the QLogic documentation.
2. Use QLogic SANsurfer to set the IP address for the HBA as described in the documentation provided with the HBA.

If the HBA is a replacement for a previously installed HBA, assign it the same IP address as the HBA it replaced, so that it automatically

has the same iSCSI initiator settings and optional CHAP security settings as the HBA it replaced.

Configuring NIC or iSCSI HBA initiators

Before an iSCSI initiator can send data to or receive data from the storage system, you must configure the initiator network parameters for the NIC or HBA initiators so that they connect with the storage-system SP iSCSI targets.

Depending on your configuration, refer to the appropriate section listed below.

- ◆ *Configuring Linux NIC initiators to connect to storage-system iSCSI targets*, page 10
- ◆ *Configuring HBA initiators to connect to the storage-system iSCSI targets*, page 15

Configuring Linux NIC initiators to connect to storage-system iSCSI targets

Each server connected to an iSCSI storage system must have a unique iSCSI initiator name for its NICs. To determine a server's iSCSI initiator name for its NICs, use `cat /etc/iscsi/initiatorname.iscsi` for open-iscsi drivers or `/etc/initiatorname.iscsi` for the sfnet drivers. If multiple servers connected to the storage system have the same iSCSI initiator name, contact your Linux provider for help on making the names unique.

Use the iSCSI driver bundled with the Linux kernel to configure the network parameters for each NIC that needs access to the storage system.



CAUTION

The Linux iSCSI driver gives the same name to all NICs in a server. This name identifies the server, not the individual NICs. This means that if multiple NICs from the same server are connected to an SP on the same subnet, then only one NIC is actually used. Other NICs are in standby mode. The server will use one of the others if the first NIC fails.

Configuring the iscsi_sfnet driver

IMPORTANT

Refer to the *EMC Linux iSCSI Attach Release Notes (P/N 300-002-672)* for the latest information on configuring the iscsi_sfnet driver.

1. For an existing storage system with initiator CHAP already configured, stop the iSCSI service:

```
/etc/init.d/iscsi stop
```

2. Open the `/etc/iscsi.conf` file on your server with vi or another editor.
3. Define a discovery address and uncomment (remove the # symbol) before the recommended variable settings in the iSCSI driver configuration file as listed in Table 2 for the Linux 2.6 kernel or Table 3 for the Linux 2.4 kernel.

Table 2 Linux 2.4 kernel iscsi_sfnet driver recommended settings

RHEL 3.0 U5 or higher updates and SuSE 8 SP4 or higher service packs (Linux 2.4 kernel)		
Variable Name	Default settings	Recommended settings
Discovery Address ^a		<i>IP address of storage system's iSCSI port</i>
HeaderDigest	prefer off	never
DataDigest	prefer off	never
PortalFailover ^b	ye	no
Multipath ^b	no	yes (when EMC PowerPath or DM-MPIO is installed) no (when EMC PowerPath or DM-MPIO is <i>not</i> installed)
DiskCommandTimeout	infinite (0 seconds)	10 <i>(Should only be changed in SLES 8 SP4 and RHEL 3.0 U5)</i>
Continuous	yes	no
ConnFailTimeout ^c	infinite (0 seconds)	15
InitialR2T	no	yes

^a In order for the parameters in the configuration file to have a global effect on the iSCSI targets, The Discovery Address list must be located as the last items in the file. For the IP addresses, refer to the iSCSI target and initiator port network information worksheet, which should have been completed when you planned your configuration.

RHEL 3.0 U5 or higher updates and SuSE 8 SP4 or higher service packs (Linux 2.4 kernel)		
Variable Name	Default settings	Recommended settings
^b These parameters are not available in RHEL 4 U3 and higher		
^c It is recommended that LoginTimeout be set to a lesser value than ConnFailTimeout by a factor of 4 to 1 in RHEL 4.0 U3 and higher updates when EMC PowerPath or the Linux native DM-MPIO is installed. Set: LoginTimeout=30; ConnFailTimeout=120.		

Table 3 Linux 2.6 kernel iscsi_sfnet driver recommended settings

RHEL 3.0 U5 or higher updates, SuSE 8 SP4 and Asianux 1.0 SP1 or higher service packs (Linux 2.6 kernel)		
Variable Name	Default settings	Recommended settings
Discovery Address ^a		<i>IP address of storage system's iSCSI port</i>
HeaderDigest	prefer off	never
DataDigest	prefer off	never
PortalFailover	yes	no
Multipath	no	yes (when EMC PowerPath or DM-MPIO is installed) no (when EMC PowerPath or DM-MPIO is <i>not</i> installed)
Continuous	yes	no
ConnFailTimeout ^b	infinite (0 seconds)	15 <i>(Should only be changed in RHEL 3.0 U6)</i>
InitialR2T	no	yes
^a In order for the parameters in the configuration file to have a global effect on the iSCSI targets, The Discovery Address list must be located as the last items in the file. For the IP addresses, refer to the iSCSI target and initiator port network information worksheet, which should have been completed when you planned your configuration.		
^b It is recommended that LoginTimeout be set to a lesser value than ConnFailTimeout by a factor of 4 to 1 in RHEL 4.0 U3 and higher updates when EMC PowerPath or the Linux native DM-MPIO is installed. Set: LoginTimeout=30; ConnFailTimeout=120.		

Any other changes to the non-CHAP part of the configuration file are not supported.

4. For an existing storage system with initiator CHAP already configured, configure CHAP for the NIC initiator as described in the section on setting up optional CHAP security.
5. After you edit the configuration file, start the iSCSI service:

```
/etc/init.d/iscsi start
```

To stop the iSCSI service, enter **/etc/init.d/iscsi stop**.

6. Set the run levels for the iSCSI service to start automatically on reboot and shutdown:

Red Hat or Asianux
chkconfig - -level 345 iscsi on

SuSE
chkconfig -s iscsi 345
chkconfig -s iscsi on

Configuring the open-iscsi driver

IMPORTANT

Refer to the *EMC Linux iSCSI Attach Release Notes* (P/N 300-002-672) for the latest information on configuring the open-iscsi driver.

The open-iscsi persistent configuration is implemented as a DBM database and contains two tables — discovery (**discovery.db**) and node (**node.db**). These iSCSI database files are located in **/etc/iscsi/**.

1. For an existing storage system with initiator CHAP already configured, stop the iSCSI service:

Red Hat
/etc/init.d/iscsi stop

SuSE
/etc/init.d/open-iscsi stop

2. Open the **/etc/iscsi/iscsid.conf** file on your server with vi or another editor.
3. Uncomment (remove the # symbol) before the recommended variable settings in the iSCSI driver configuration file as listed in Table 4.

Table 4 Open-iscsi driver recommended settings

RHEL 5 or higher updates and SuSE 10 or higher (Linux 2.6 kernel)		
Variable Name	Default settings	Recommended settings
node.startup	manual	auto
node.session.iscsi.InitialR2T	No	Yes
node.session.iscsi.ImmediateData	Yes	No
node.session.timeo.replacement_timeout	120	60 ^a
node.conn[0].timeo.timeo.noop_out_interval	10	<i>Higher in congested networks^b</i>
node.conn[0].timeo.timeo.noop_out_timeout	15	<i>Higher in congested networks^b</i>
^a When using multipathing software, such as EMC's PowerPath or the native Linux DM-MPIO, you may decrease this time to 30 seconds for a faster failover. However, this timer <i>must</i> be greater than the node.conn[0].timeo.timeo.noop_out_interval and node.conn[0].timeo.timeo.noop_out_timeout times combined.		
^b This value should <i>not</i> exceed the value in node.session.timeo.replacement_timeout.		

4. Set the run levels for the iSCSI service to start automatically on reboot and shutdown:

Red Hat

chkconfig - -level 345 iscsid on

SuSE

chkconfig -s open-iscsi 345

chkconfig -s open-iscsi on

5. If you are running Red Hat 5 or higher, configure the targets you wish to connect to using the **iscsiadm** command. For information on the **iscsiadm** command and its syntax, refer to the manpages.
 - a. Discover the targets you want your server to connect to. You only need to perform a discovery on a single IP address and the storage system will return all the configured iSCSI targets.

iscsiadm -m discovery -t st -p target_ip_address

- b. Log in to the target.

iscsiadm -m node -L all

6. If you are running SuSE 10 or higher, configure the targets you wish to connect to using the YaST™ utility.
 - a. Open the YaST utility.
 - b. Select **Network Services > iSCSI Initiator > iSCSI Initiator Overview**.
 - c. Select the **Service** tab and note the initiator name and select a service start time (boot or manual).
 - d. Select the **Discovered Targets** tab and click **Discovery**.
 - e. Enter one of the target IP address and select **No Authentication**, then click **Next**.

You will enable CHAP authentication later.

The utility displays all the configured iSCSI targets.

- f. Select the targets you want to log in to.
- g. Click **Finish**.

Configuring HBA initiators to connect to the storage-system iSCSI targets

Use the QLogic SANsurfer software to configure the network parameters for each QLogic iSCSI HBA that needs to access the storage system.

For PowerPath to work, each iSCSI HBA must be on a separate subnet.

1. Open QLogic SANsurfer as described in the QLogic documentation.
2. For each iSCSI connection to the storage system:
 - a. If multiple HBAs are listed in the first column under the server's name, select the HBA to be configured.
 - b. Click the **Target Settings** tab.
 - c. On the **Target Settings** page, click the green plus (+) sign and enter the IP address for the iSCSI port on your storage system, and click **OK**.

For the iSCSI data port IP addresses, refer to the iSCSI target and initiator port network information worksheet, which should have been completed when you planned your configuration.

The state for the port is `No Connection Active`.

- d. Select **Auto Discover Targets**.
- e. Click **Save** and **Yes** to save the changes and discover all targets.

If the network is routed, the discovery finds all targets (ports) for the IP address you entered earlier. The state of routed ports is `Session Active`; for unrouted ports, it is `Unknown`.

- f. In the **Security Check** window, enter your password and click **OK**.

The default password is **config**.

For an existing storage system with CHAP already configured, the state will be `Session Failed`.

- g. For an existing storage system with CHAP already configured:
 - ♦ Configure CHAP for the iSCSI HBA initiator as described in the section on setting up optional CHAP security.
 - ♦ After you enable CHAP security for the iSCSI HBA initiator, click **Save**.
 - ♦ At the prompt to refresh the information for the server, click **Yes**.
- h. Select **Config Parameters**.
- i. Select and enable all the targets that you want to connect to the server.

If you do *not* want the server to connect to a port or you want to remove unknown ports, select the entry for the port and click the red minus (-) sign.

- j. Enable timestamps, set the execution throttle to 256, and uncheck immediate data.
- k. Click **Save** and **Yes**.

1. In the **Security Check** window, enter your password and click **OK**.

The HBA performs an iSCSI discovery. Once finished, SANsurfer displays all targets on the storage system.

3. To configure the BIOS settings, refer to the EMC iSCSI QLogic Host Bus Adapters for Linux, which is available on the [Powerlink](#) website.

Preparing for CHAP security

To prepare for using CHAP security, you must have done the following:

- ❑ Completed the CHAP worksheets in the chapter on iSCSI configuration in the appropriate configuration and planning guide that either shipped with your storage system or that you generated from the customized storage-system support website.

Configuring CHAP on the iSCSI initiators

Before configuring CHAP security on iSCSI initiators, verify that you have completed the steps listed in the previous section, *Preparing for CHAP security*.

To configure initiator CHAP, refer to one of the following sections:

- ◆ *Configuring initiator CHAP on NIC initiators on a Linux server*, page 19
- ◆ *Configuring initiator CHAP on the iSCSI HBA initiators on a server*, page 26

Navisphere Express refers to initiator CHAP as *basic* CHAP.

To configure mutual CHAP (optional), refer to one of the following sections:

- ◆ *Configuring mutual (target) CHAP on NIC initiators on a Linux server*, page 27
- ◆ *Configuring mutual (target) CHAP on the iSCSI HBA initiators on a server*, page 30

Navisphere Express refers to mutual CHAP as *advanced* CHAP.

Configuring initiator CHAP on NIC initiators on a Linux server



CAUTION

You must enable CHAP security for the NIC or iSCSI HBA *before* you can configure CHAP on the storage system. While you are setting up and enabling CHAP, you may temporarily lose connectivity between the server and the storage system.

After entering CHAP data on the target, you must enter the same data on each NIC initiator. On each initiator, you enter the initiator CHAP user account data (username and secret) that the initiator sends to the target for authentication. For initiator CHAP, this data is the initiator

username and secret that you entered on the target. When the initiator sends this data, the target compares it with an account database and authenticates the initiator.

Enabling initiator CHAP for the `iscsi_sfnet` driver

1. Start the Linux iSCSI driver by typing `/etc/init.d/iscsi start`.
2. Based on the security model you want to build for security, follow the examples in the `/etc/iscsi.conf` configuration file to define usernames and passwords.
3. Find the driver parameter models you want to use, and configure them as shown in the examples in configuration file.

For more configuration information and examples, see the README file in the source directory.

The following excerpt from the `iscsi.conf` configuration file shows two sections of the file: the Authentication Settings section and the Target Name Specific Settings section. The Authentication Settings section shows an authenticated configuration using CHAP. The Target Name Specific Settings section shows a non-authenticated configuration.

Your version of `iscsi.conf` may be different from the file shown below. This example shows some configuration guidelines.

```
# iSCSI configuration file - see iscsi.conf(5)
# Authentication Settings
# ----- #
# You may configure a default Username and Password to
# use for CHAP
# authentication by specifying the Global username and
# password parameters
# in the format as mentioned below. These entries will
# need to precede any
# "DiscoveryAddress" entries if authentication needs to
# be enabled for all the
# iSCSI targets.
#
# Example:
#
# Username=john
# Password=welcome
# or
```

```

# OutgoingUsername=john
# OutgoingPassword=welcome
#
# The "OutgoingUsername" will specify the username to
# be sent to the target
# for login authentication. The "OutgoingPassword" is
# the CHAP secret password
# to be used when sending challenge responses to the
# target.
#
# You may configure CHAP authentication settings that
# will apply to every
# target discovered at a particular address by adding
# "OutgoingUsername=u"
# and "OutgoingPassword=p" entries indented below the
# "DiscoveryAddress"
# entry they apply to.
#
# Example:
#DiscoveryAddress=127.0.0.1      (Storage System1 SPA)
#  Username=john
#  Password=welcome
#DiscoveryAddress=127.0.0.2      (Storage System1 SPB)
#  Username=betty
#  Password=bienvenue
#
#           or
#DiscoveryAddress=127.0.0.1      (Storage System1 SPA)
#DiscoveryAddress=127.0.0.2      (Storage System1 SPB)
#DiscoveryAddress=127.0.00.1     (Storage System2 SPA)
#DiscoveryAddress=127.0.00.2     (Storage System2 SPB)
#  Username=john
#  Password=welcome
#DiscoveryAddress=127.0.0.3      (Storage System3 SPA)
#DiscoveryAddress=127.0.00.3     (Storage System3 SPB)
#  Username=betty
#  Password=bienvenue
#
# You can configure 2 WAY authentication to enable the
# authentication of the
# initiator by the target and vice-versa. The "Outgoing
# Username" and "Outgoing
# Password" fields specify the initiator authentication
# and "IncomingUsername"
# and "IncomingPassword" can be used for target
# authentication.
#
# The "IncomingUsername" will specify the username that
# must be received from
# target if login authentication occurs. The
# "IncomingPassword" is the CHAP
# secret to be used when verifying challenge responses
# from the target.
# The "OutgoingPassword" and "IncomingPassword" fields
# should be unique.
#
# Example:
#
# OutgoingUsername=alice
# OutgoingPassword=foo
#
# IncomingUsername=alice3

```

```

# IncomingPassword=foo
# TargetName Specific Settings
# -----
# Target-specific settings should be entered below the
# respective "TargetName"
# entries. If Multipath is enabled, then these
# target-specific settings will be
# be applicable for all iSCSI sessions to this target.
#
# If settings under "Subnet" entry are conflicting with
# settings under
# "TargetName" entry, the settings under "Subnet" will
# be considered.
#
#TargetName=iqn.1987-05.com.cisco:00.0d1d898e8d66.t0
#
# The TargetName Settings can have the following entries
# specific to a target.
#
# 1) CRC Settings
# 2) iSCSI Operational Parameter
# settings
# 3) Connection Timeout Settings
# 4) Session Timeout Settings
# 5) Error Handling Timeout Settings
# 6) TCP Settings
# 7) Portal Failover Settings
# 8) Multipath Settings
# 9) LUN settings
# 10) PreferredSubnet and PreferredPortal Settings
# NOTES:
# -----
# If any of the configuration parameters are not
# mentioned under Configuration
# type DiscoveryAddress, TargetName or Subnet, global
# values will be
# considered if they are specified, else default
# settings will apply for these
# configuration parameters.
#
# All entries specified below any of the Configuration
# types must be indented
# by a whitespace character or a tab to be considered
# local to a category. If
# they are specified in the 1st column they are by
# default considered as global
# values.
#
# Example: #
#Subnet=127.0.0.1
#   ActiveTimeout=10
#   PingTimeout=10
#   LoginTimeout=30
#
# In the above case LoginTimeout is considered a global
# value and will have
# scope until another LoginTimeout entry is specified.
# If there are conflicting entries for the same target
# through the Subnet and
# TargetName or DiscoveryAddress entries, the Subnet
# entries in the file will
# take precedence.

```

```

#
# Example:
#
#Subnet=127.0.0.1
#  ActiveTimeout=10
#
#TargetName=ign.1987-05.com.cisco:00.0d1d898e8d66.t0
#  ActiveTimeout=15
#
# In the above scenario, the Subnet specific setting
#   will take effect.
# If there is any conflict between DiscoveryAddress
#   and Global entries,
# DiscoveryAddress settings takes precedence.
#
#Username=bob
#Password=bob123
# DiscoveryAddress=127.0.0.1
#   Username=
#   Password= DiscoveryAddress=127.0.0.2
#   Username=
#   Password= DiscoveryAddress=127.0.0.3
#   Username=
#   Password= DiscoveryAddress=127.0.0.4
#   Username=
#   Password=
#   DiscoveryAddress=127.0.0.5
#   Username=
#   Password= DiscoveryAddress=127.0.0.6
#   Username=
#   Password=
# In the above case, the DiscoveryAddress settings
#   will be considered.
# Targets without any matching Subnet, TargetName or
#   DiscoveryAddress entries
# will take the global values if any in the config file,
#   else the default
# values will take effect.
#
# Example:
#
#HeaderDigest=prefer-on
#DataDigest=prefer-on
#InitialR2T=No
#ActiveTimeout=10
#
# If there are any duplicate entries for a configuration
#   parameter in the conf
# file the latest entry in the file will take effect.
#
# Example:
#
# IncomingUsername=alice
# IncomingPassword=alice123
#multipath=no
#LUNs=0-255
# IncomingUsername=bob
# IncomingPassword=bob123
#
# In the above case, IncomingUsername will be "bob"
#   and IncomingPassword will
# be "bob123".

```

#

When you have configured initiator CHAP for each NIC initiator in the server, you have set and enabled initiator security on the server and storage system.

4. Restart the iSCSI service:

```
/etc/init.d/iscsi stop  
/etc/init.d/iscsi start
```

5. Run the Navisphere Server Utility to update the storage system with the server information.

Enabling initiator CHAP for the open-iscsi driver

1. Start the Linux iSCSI driver.

```
Red Hat  
/etc/init.d/iscsi start
```

```
SuSE  
/etc/init.d/open-iscsi start
```

2. If you are running Red Hat 5 or higher, configure CHAP security on the open-iscsi driver initiator using the **iscsiadm** command. For information on the **iscsiadm** command and its syntax, refer to the manpages.
 - a. Enable CHAP using the **iscsiadm** command.

```
iscsiadm -m node -r $recid -o update -n  
node.session.auth.authmethod -v CHAP
```

- b. Set the user name on the initiator.

```
iscsiadm -m node -r $recid -o update -n  
node.session.auth.username -v user_name
```

- c. Set the secret key on the initiator.

```
iscsiadm -m node -r $recid -o update -n  
node.session.auth.password -v password
```

3. If you are running SuSE 10 or higher, configure CHAP security on the open-iscsi driver initiator using the YaST™ utility.
 - a. Open the YaST utility.
 - b. Select **Network Services > iSCSI Initiator > iSCSI Initiator Overview**.
 - c. Select the **Connected Targets** tab and select the initiator you want to set initiator CHAP authentication for.
 - d. Click **Add**.
 - e. Select the **Incoming Authentication** (initiator CHAP) and enter the username and password.
 - f. Click **Next**.
 - g. Repeat steps c – f for each NIC initiator in the server you want to configure initiator CHAP.
 - h. Click **Finish**.
4. Find the driver parameter models you want to use, and configure them as shown in the examples in configuration file.
5. Restart the iSCSI service.

```
Red Hat  
/etc/init.d/iscsi stop  
/etc/init.d/iscsi start
```

```
SuSE  
/etc/init.d/open-iscsi stop  
/etc/init.d/open-iscsi start
```

6. Run the Navisphere Server Utility to update the storage system with the server information.

Configuring initiator CHAP on the iSCSI HBA initiators on a server



CAUTION

You must enable CHAP security for the NIC or iSCSI HBA *before* you can configure CHAP on the storage system. While you are setting up and enabling CHAP, you may temporarily lose connectivity between the server and the storage system.

Configure initiator CHAP on *each* iSCSI HBA that communicates with the server.

The steps below apply to version 4.01.00 or later of the QLogic SANsurfer software. If you are running an earlier version, refer to the SANsurfer documentation.

The SANsurfer diagnostic read/write buffer test is *not* supported with CLARiiON storage systems.

1. Open the SANsurfer software.
2. Click **Connect** and enter the hostname or IP address. Click **Connect**.
3. Under the **iSCSI HBA** tab, double-click the HBA and select the HBA port.
4. Click the **Target Settings** tab.
5. Click **Config Authentication** on the bottom of the pane.

The default password is **config**.

6. Select the **CHAP** tab.
7. Click the green plus sign (+) on the right of the **CHAP Entries** portion of the **CHAP** screen.
 - a. Type in the initiator name for your HBA initiator. This name must match the CHAP username you entered on the storage system.

- b. Type in the secret for that initiator. The CHAP username secret must match the secret you entered on the storage system.
 8. Under the **Targets** portion of the **CHAP** screen, select the **Chap Name/Secret** row; then from the drop-down menu, select the initiator name and secret you just entered in the **CHAP Entries** table.
 9. Click **OK**.
 10. Save your changes on the **Target Settings** window (the default password remains **config**).
- You have set up initiator CHAP security on the server.

Configuring mutual (target) CHAP on NIC initiators on a Linux server



CAUTION

You must enable CHAP security for the NIC or iSCSI HBA *before* you can configure CHAP on the storage system. While you are setting up and enabling CHAP, you may temporarily lose connectivity between the server and the storage system.

After entering CHAP data for the NIC initiators, you must enter the same data on the target.

Enabling mutual (target) CHAP for the `iscsi_sfnet` driver

1. Open the `/etc/iscsid.conf` file on your server with `vi` or another editor.
2. For each NIC initiator in the server, enter the initiator CHAP user account data (username and secret) that the initiator sends to the target for authentication.

This data is one of the initiator usernames and secrets that you entered on the target. When the initiator sends this data, the target compares it with an account database and authenticates the initiator.

The following example in the Authentication Settings section of the `iscsi.conf` file shows mutual (advancedtarget) CHAP.

```
Username=john
```

```
Password=welcome
  or
OutgoingUsername=john
OutgoingPassword=welcome
```

The following example in the Authentication Settings section of the **iscsid.conf** file shows mutual (advancedtarget) CHAP, which lets you set different usernames and secrets for each host initiator. The first part shows one storage system; each SP has a different username and password. The second part shows three storage systems; two use one username and password, and the third uses a different username and password.

```
DiscoveryAddress=127.0.0.1          (Storage System1 SPA)
  Username=john
  Password=welcome
DiscoveryAddress=127.0.0.2          (Storage System1 SPB)
  Username=betty
  Password=bienvenue
#
#                               or
DiscoveryAddress=127.0.0.1          (Storage System1 SPA)
DiscoveryAddress=127.0.0.2          (Storage System1 SPB)
DiscoveryAddress=127.0.0.3          (Storage System2 SPA)
DiscoveryAddress=127.0.0.4          (Storage System2 SPB)
  Username=john
  Password=welcome
DiscoveryAddress=127.0.0.5          (Storage System3 SPA)
DiscoveryAddress=127.0.0.6          (Storage System3 SPB)
  Username=betty
  Password=bienvenue
```

When you have configured mutual (advancedtarget) CHAP for each NIC initiator in the server, you have completed the setup and enabling of security on the server and storage system.

3. Restart the iSCSI service:

```
Red Hat
/etc/init.d/iscsi stop
/etc/init.d/iscsi start
```

```
SuSE
/etc/init.d/open-iscsi stop
/etc/init.d/open-iscsi start
```

4. Run the Navisphere Server Utility to update the storage system with the server information.

Enabling mutual (target) CHAP for the open-iscsi driver

1. Start the Linux iSCSI driver.

Red Hat
`/etc/init.d/iscsi start`

SuSE
`/etc/init.d/open-iscsi start`

2. If you are running Red Hat 5 or higher, configure mutual CHAP security on the open-iscsi driver initiator using the **iscsiadm** command. For information on the **iscsiadm** command and its syntax, refer to the manpages.
 - a. Enable CHAP using the **iscsiadm** command.

```
iscsiadm -m node -r $recid -o update -n  
node.session.auth.authmethod -v CHAP
```

- b. Set the user name on the initiator.

```
iscsiadm -m node -r $recid -o update -n  
node.session.auth.username -v user_name
```

- c. Set the secret key on the initiator.

```
iscsiadm -m node -r $recid -o update -n  
node.session.auth.password -v password
```

3. If you are running SuSE 10 or higher, configure CHAP security on the open-iscsi driver initiator using the YaST™ utility.
 - a. Open the YaST utility.
 - b. Select **Network Services > iSCSI Initiator > iSCSI Initiator Overview**.
 - c. Select the **Connected Targets** tab and select the initiator you want to set initiator CHAP authentication for.
 - d. Click **Add**
 - e. Select the **Outcoming Authentication** (mutual CHAP) and enter the username and password.
 - f. Click **Next**.

- g. Repeat steps c – f for each NIC initiator in the server you want to configure mutual CHAP.
 - h. Click **Finish**.
4. Find the driver parameter models you want to use, and configure them as shown in the examples in configuration file.
 5. Restart the iSCSI service.

```
Red Hat
/etc/init.d/iscsi stop
/etc/init.d/iscsi start
```

```
SuSE
/etc/init.d/open-iscsi stop
/etc/init.d/open-iscsi start
```

6. Run the Navisphere Server Utility to update the storage system with the server information.

Configuring mutual (target) CHAP on the iSCSI HBA initiators on a server



CAUTION

You must enable CHAP security for the NIC or iSCSI HBA *before* you can configure CHAP on the storage system. While you are setting up and enabling CHAP, you may temporarily lose connectivity between the server and the storage system.

Mutual CHAP is applied *in addition to* initiator CHAP, so you must set up initiator CHAP *before* setting up mutual CHAP.

The steps below apply to version 4.01.00 or later of the QLogic SANsurfer software. If you are running an earlier version, refer to the SANsurfer documentation.

The SANsurfer diagnostic read/write buffer test is *not* supported with CLARiiON storage systems.

1. Open the SANsurfer software.
2. Click **Connect** and enter the hostname or IP address, and click **Connect**.
3. Under the **iSCSI HBA** tab, double-click the HBA and select the HBA port.
4. Select the **Target Settings** tab.
5. Select **Config Authentication** from the bottom of the pane, and in the password prompt, use the password **config**.
6. Select the **CHAP** tab.
7. Click the green plus sign (+) on the right of the **Target Table** portion of the **CHAP** screen.
 - a. In the blank row under the **Target Name** column, enter the *target* CHAP username that you entered on the storage system.
 - b. In the **Target Secret** column, enter the *target* CHAP secret that you entered on the storage system.
8. Under the **Targets** portion of the **CHAP** screen, select **Bidi** (bi-directional) for the target you want the initiator to authenticate.
9. Click **OK**.
10. Save your changes on the **Target Settings** screen (the default password remains **config**).

You have set up mutual CHAP security on the server.

Modifying CHAP credentials on the server

Before modifying the CHAP secret on the server, you *must* modify it on the storage system first.

For information on modifying CHAP credentials on the storage system, refer to the Navisphere Manager or Navisphere Express online help.

Modifying the mutual CHAP secret for NICs

1. Open the `/etc/iscsid.conf` file on your server with `vi` or another editor.
2. Modify the appropriate target's outgoing username and password (initiator CHAP) or incoming username and password (mutual/target CHAP).
3. Restart the iSCSI service.

```
Red Hat
/etc/init.d/iscsi stop
/etc/init.d/iscsi start
```

```
SuSE
/etc/init.d/open-iscsi stop
/etc/init.d/open-iscsi start
```

Modifying the mutual CHAP secret for iSCSI HBAs

The SANsurfer diagnostic read/write buffer test is *not* supported with CLARiiON storage systems.

1. Open the SANsurfer software.
2. Click **Connect** and enter the hostname or IP address. Click **Connect**.
3. Under the **iSCSI HBA** tab, double-click the HBA and select the HBA port.
4. Click the **Target Settings** tab.

5. Click **Config Authentication** on the bottom of the pane.

The default password is **config**.

6. Select the **CHAP** tab.
7. Under the **Target Table** portion of the **CHAP** screen, select the target secret you want to modify and enter the new mutual CHAP secret (password). Be sure to enter the same new secret you entered on the storage system.
8. Click **OK**.
9. Save your changes on the **Target Settings** window (the default password remains **config**).

Copyright© 2006–2008 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks mentioned herein are the property of their respective owners.