nexenta
Enterprise class storage for everyone

NexentaStor

iSCSI Security Using CHAP

Nexenta Solutions Engineering Team

September 2012

Contents

iSCSI Security Using CHAP

Purpose

Securing LUNs accessed via iSCSI is accomplished by using Challenge-Handshake Authentication Protocol, or CHAP authentication. There are two flavors of CHAP authentication: unidirectional and bidirectional. The goal of this paper is to walk through the setup and understand the concepts around LUN masking in iSCSI.

iSCSI Qualified Names

iSCSI Qualified Names (IQNs) are used in the iSCSI world similar to the way World Wide Names (WWN) are used in the Fibre Channel world. IQNs should be unique in order to identify each component within the iSCSI storage network. Instead of using default IQNs, it may be easier to identify a component inside the network if named in a descriptive way. IQNs also need to be lowercased.

Examples:

iqn.2008-01.com.nexenta:target:storagetarget1

iqn.1986-03.com.sun:01:806ae8c600ff.4e97b831

iSCSI CHAP Authentication

CHAP is used in the initial stages of an iSCSI session to provide authentication between the peers on the storage network.

In iSCSI, as in other storage infrastructures, there are targets and initiators. Targets and initiators are identified by their IQNs. In addition to masking by initiator and target IQNs, CHAP offers added security. The two avenues of CHAP authentication are: one-way and mutual—also known as unidirectional and bidirectional CHAP.

Unidirectional CHAP is accomplished when a target authenticates an initiator based on the username and password the initiator sends along. This protects the target from unknown initiators connecting to its storage LUNs. The initiator receives a CHAP response to its request for authentication.

Bidirectional CHAP is accomplished by setting a username and password for a target on the initiator. This keeps the target honest, and allows the initiator to identify a rogue target on the network. This type of authentication is called bidirectional because it is combined with target-side authentication as described in the unidirectional CHAP above.

Unidirectional CHAP Implementation

In NexentaStor, unidirectional CHAP authentication is simple to set up. In the following example, we combine Target Portal Groups (TPG) with unidirectional CHAP authentication to secure our iSCSI mappings.

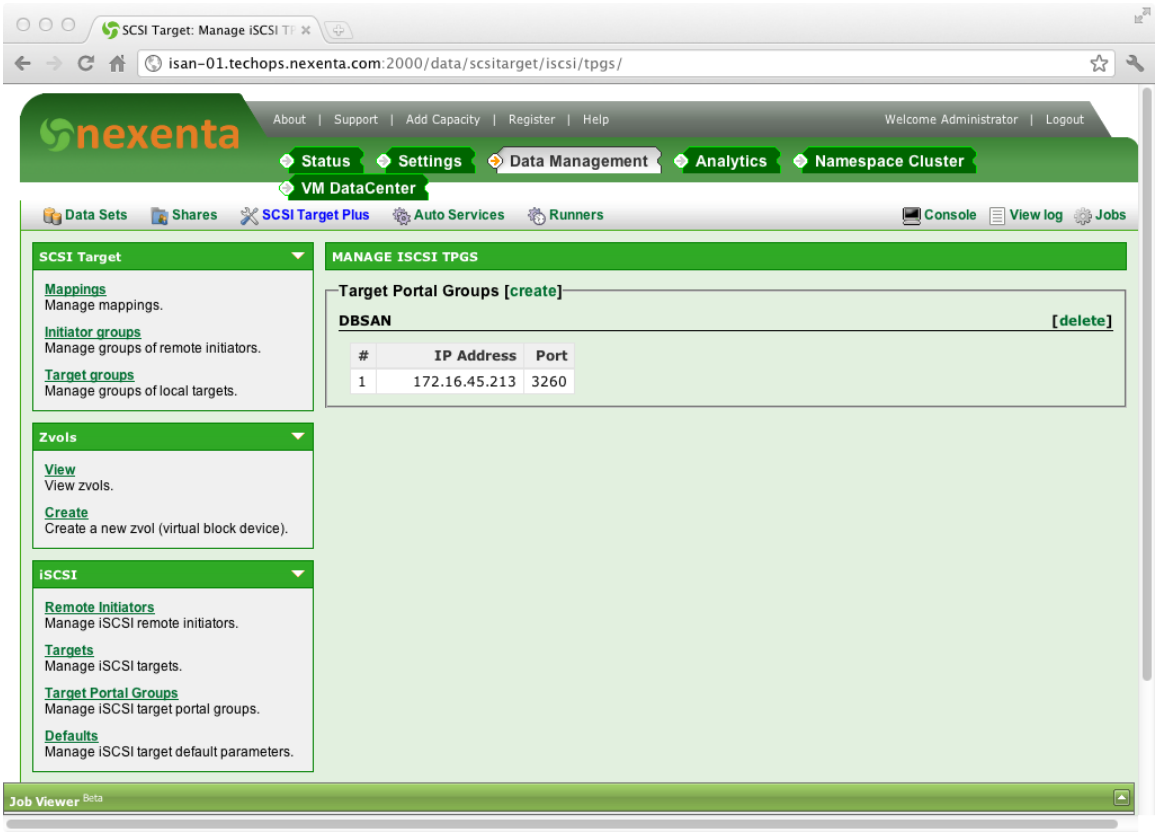

Figure 1: Create a Target Portal Group for each interface on the storage network.

In this case, we have one interface so we will use one TPG.

In the above example, click on Create next to Target Portal Groups and fill in the values.

Now that we have a TPG set up, we can create a new target. I will give the target a descriptive name and use: “iqn.2008-01.com.nexenta:target:storagetarget1”

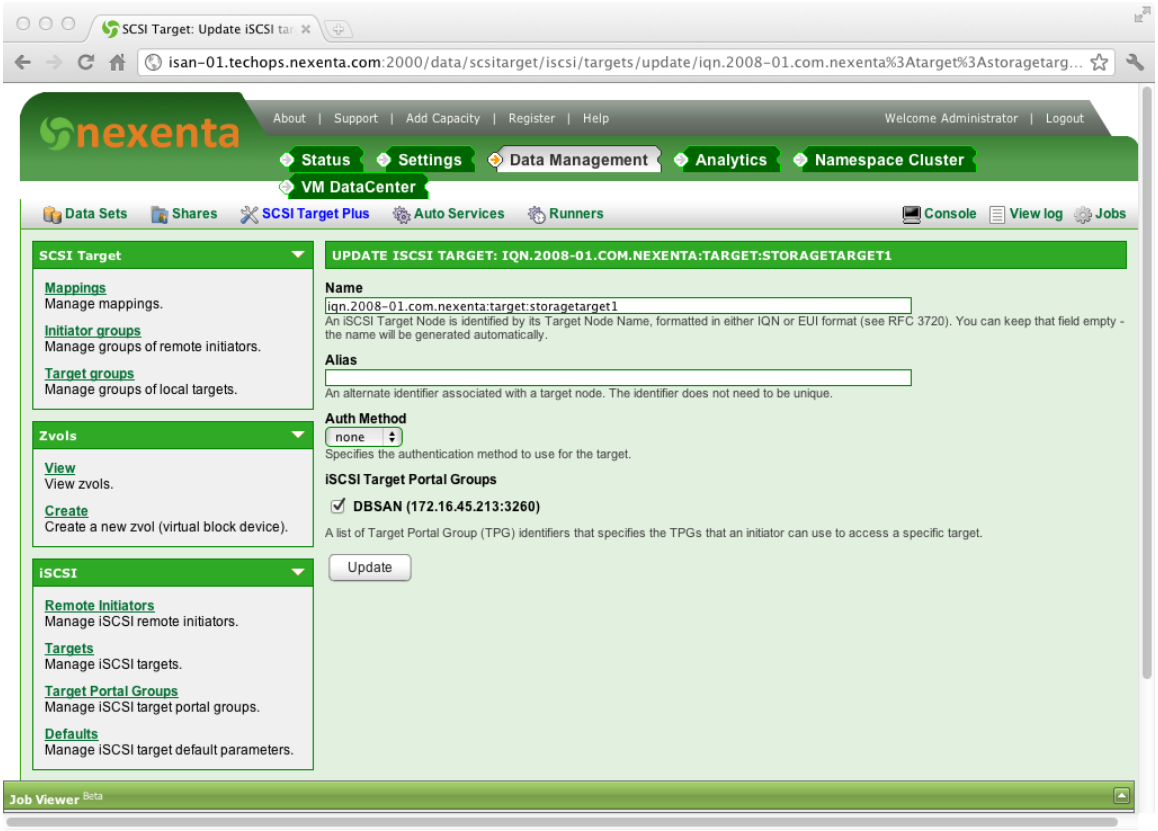

Figure 2: Leave “Auth Method” to none when creating the target.

This will be used in the next section when we discuss bidirectional CHAP authentication.

Because unidirectional CHAP is accomplished by identifying the initiator node by its CHAP username and password, we need to know the IQN of the initiator.

In this example, the initiator node is running OpenIndiana, which is based on the illumos kernel.

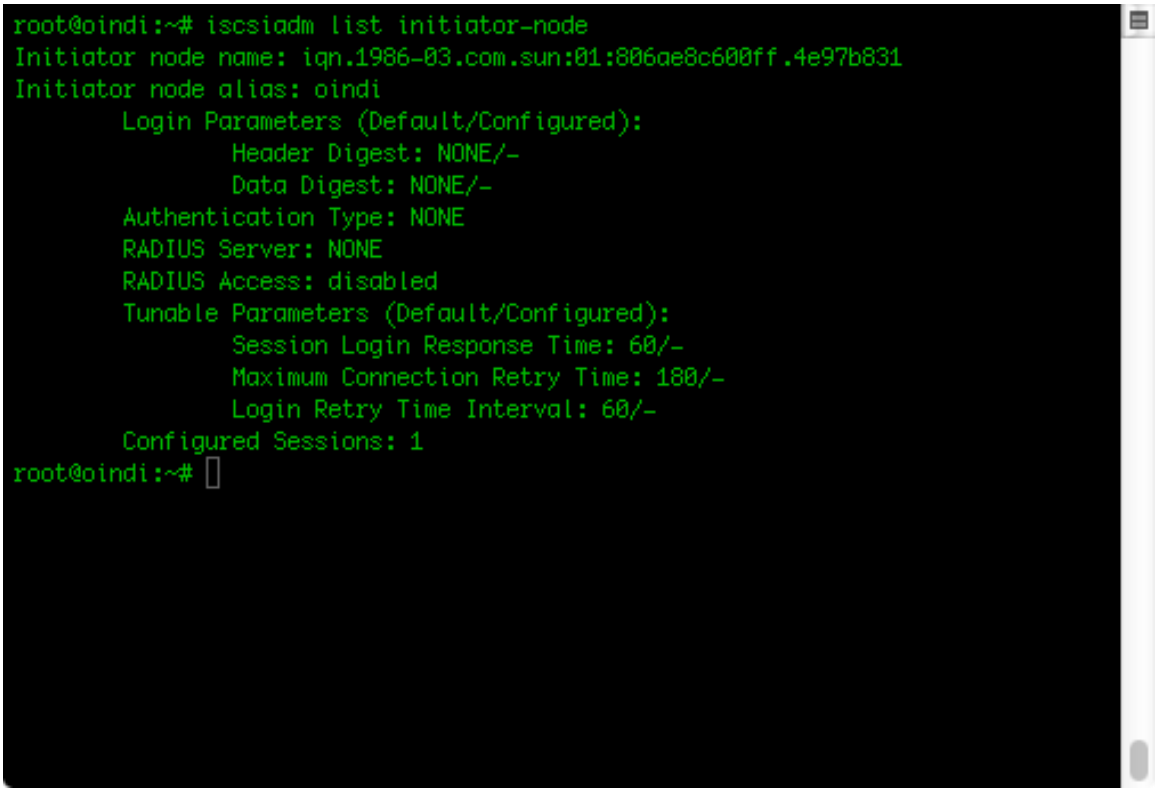

Figure 3: To acquire the IQN of the initiator, run the following command:

root@ioni: ~# iscsiadm list initiator-node

Using the initiator IQN, we create a new Remote Initiator on NexentaStor and give it a CHAP username and password (also called User and Secret).

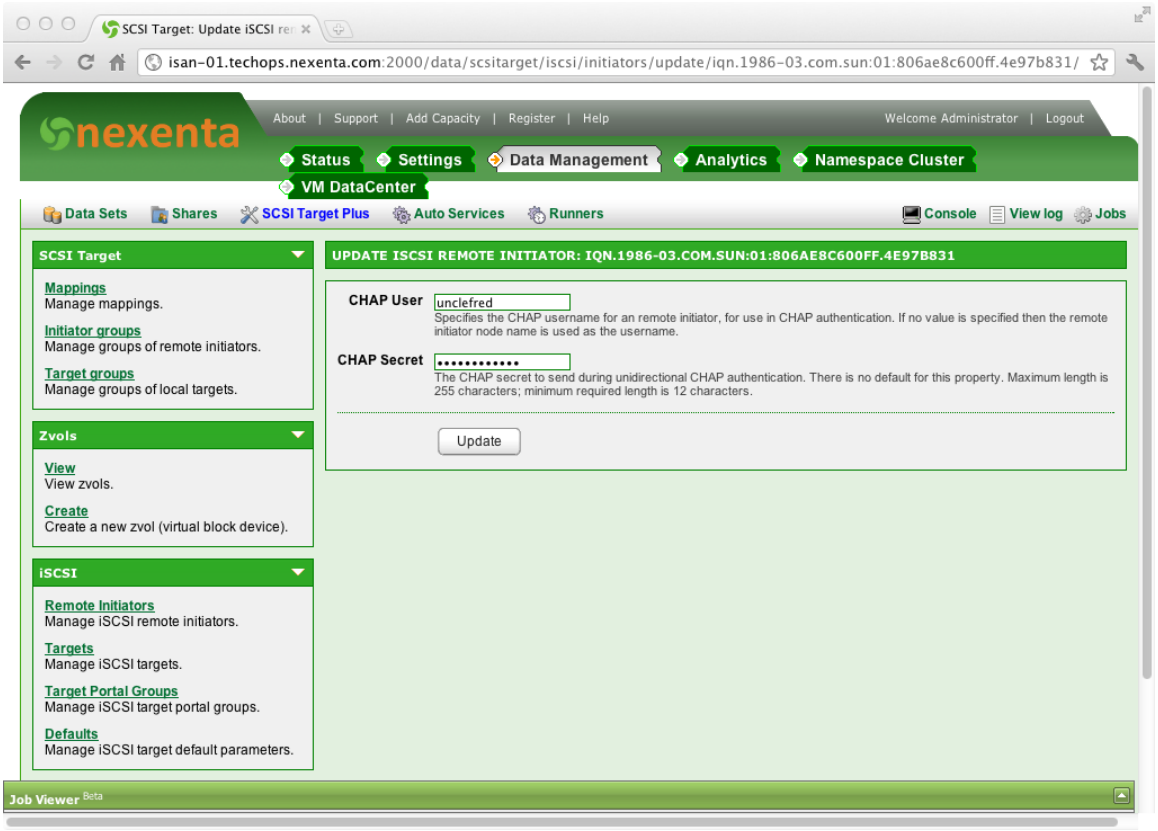

Figure 4: The CHAP user on the initiator is “unclefred”.

This is all that is required on the NexentaStor (target) side to enable unidirectional CHAP.

On the OpenIndiana initiator, CHAP User and Secret need to be setup.

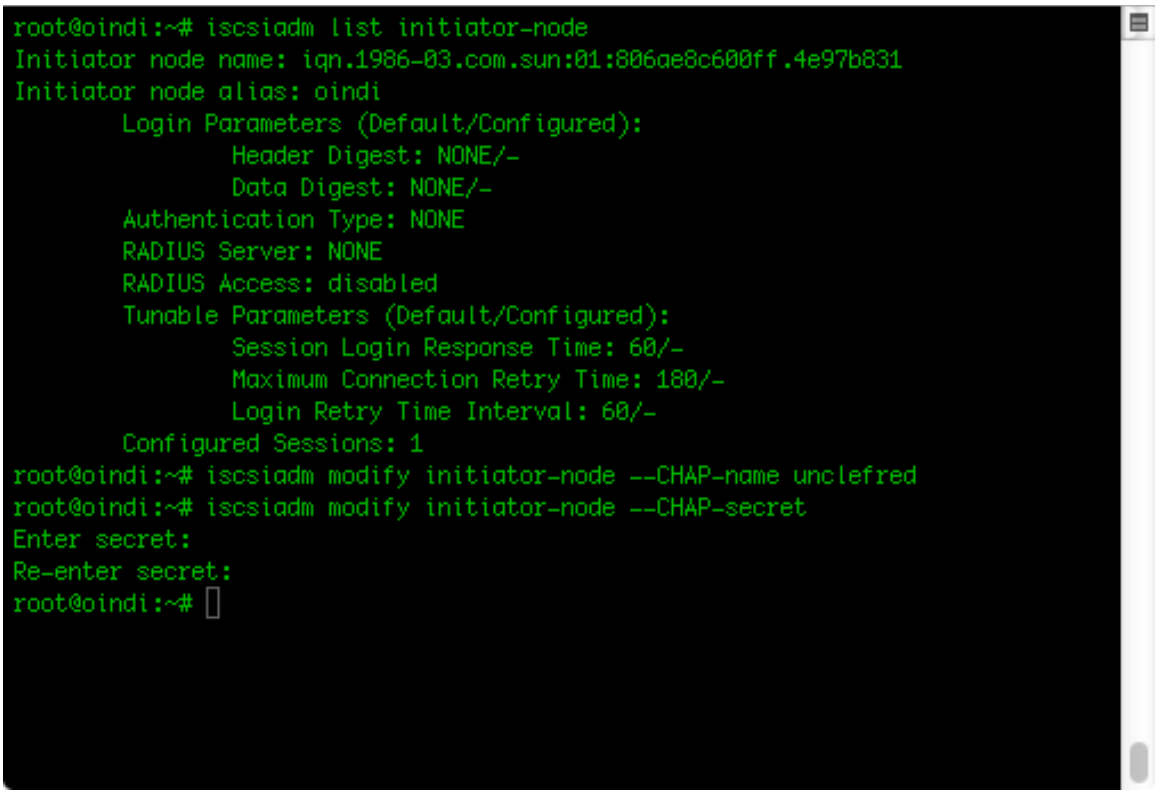

Figure 5: The initiator is configured using two commands:

root@oindi:~# iscsiadm modify initiator-node –CHAP-name unclefred

root@oindi:~# iscsiadm modify initiator-node –CHAP-secret

Once the initiator CHAP User and secret are configured, the next step is to do discovery of the target. Static discovery can be used to find LUNs available to the initiator for use.

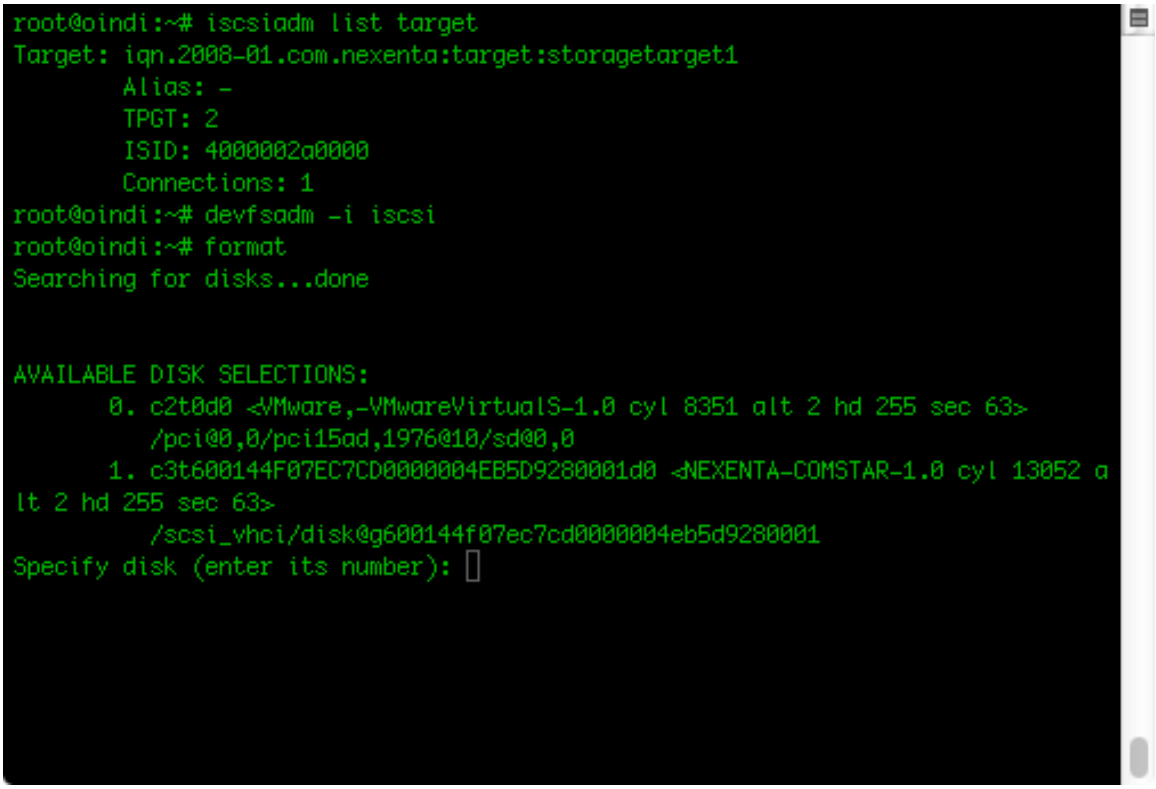

Figure 6: Finding LUNS available to the initiator using the following commands:

root@oindi:~# iscsiadm modify discovery --static enable

root@oindi:~# iscsiadm add static-config iqn.2008-

01.com.nexenta:target:storagetarget1,172.16.45.213:3260

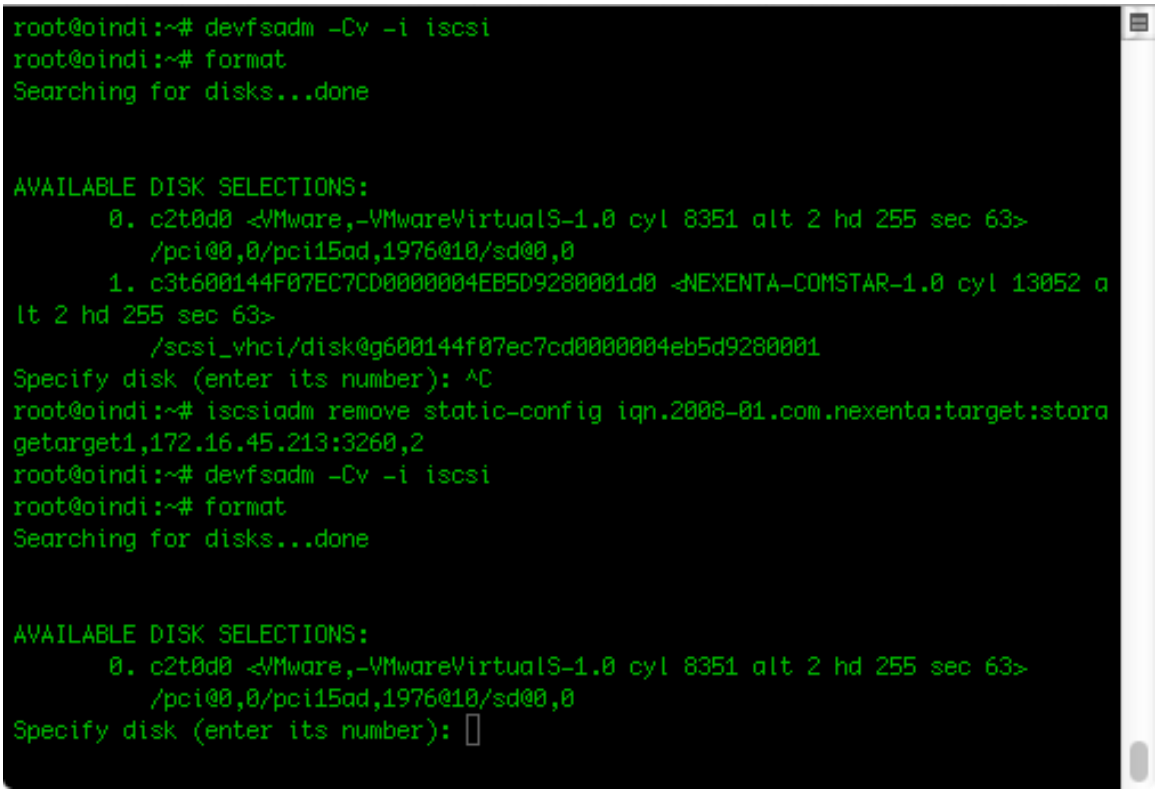

Figure 7: After the target discovery process, the following command is used to identify the new LUN:

root@oindi: ~# devfsadm –Cv –i iscsi

We then run the 'format' command and see the new device is available for use and configured for unidirectional CHAP authentication.

Bidirectional CHAP

Bidirectional CHAP now can be enabled. On NexentaStor, modify the target that already has been created in the previous unidirectional CHAP example.

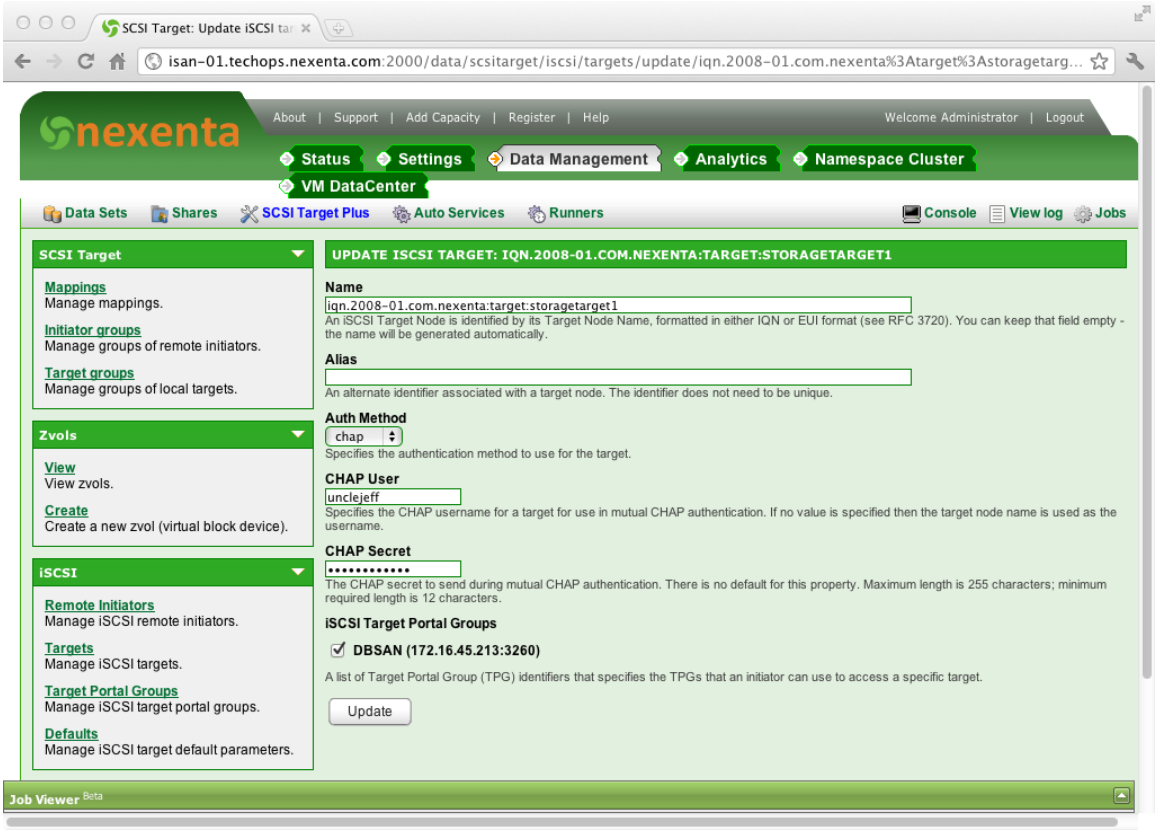

Figure 8: Auth Method will be set to CHAP, and a CHAP username and secret will be specified.

"unclejeff" will be the username for the target.

NexentaStor (target) now is ready for bidirectional CHAP

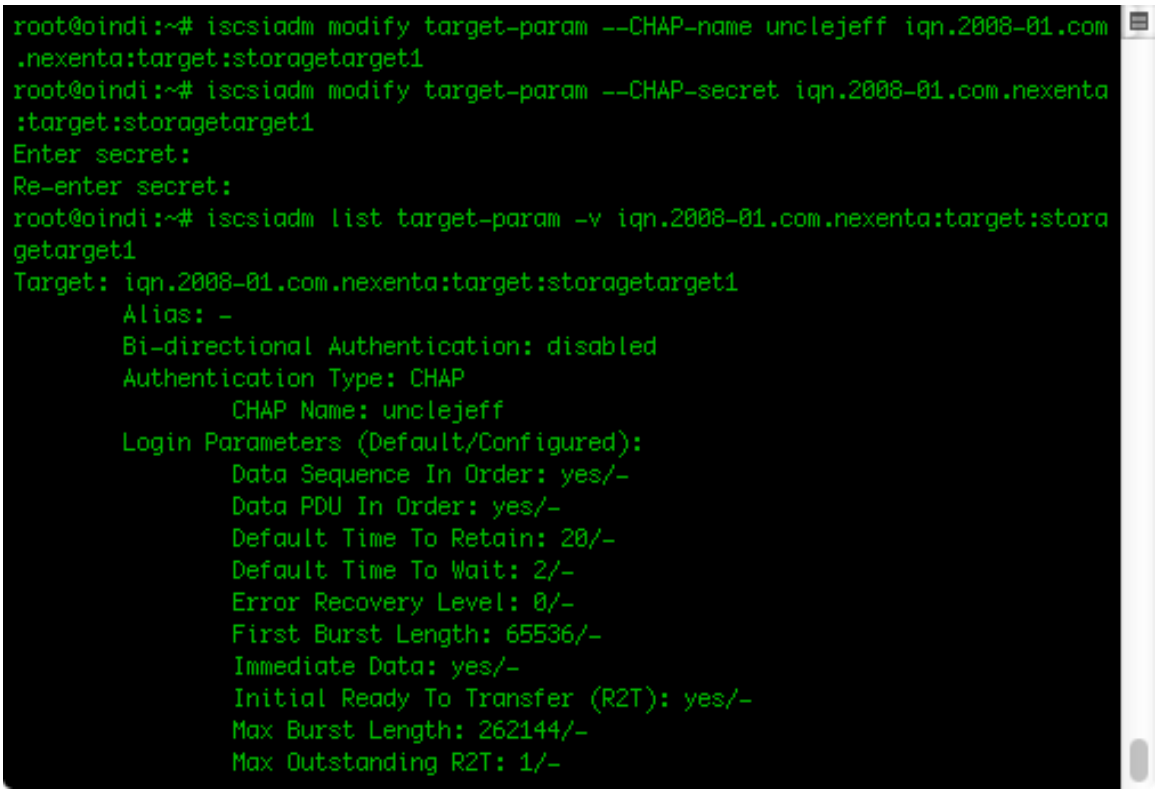

Figure 9: On the initiator, a CHAP username and secret are added to the target.

root@oindi:~# iscsiadm modify target-param –CHAP -name unclejeff iqn.2008-01.com.nexenta:target:storagetarget1

root@oindi:~# iscsiadm modify target-param –CHAP-secret iqn.2008-01.com.nexenta:target:storagetarget1

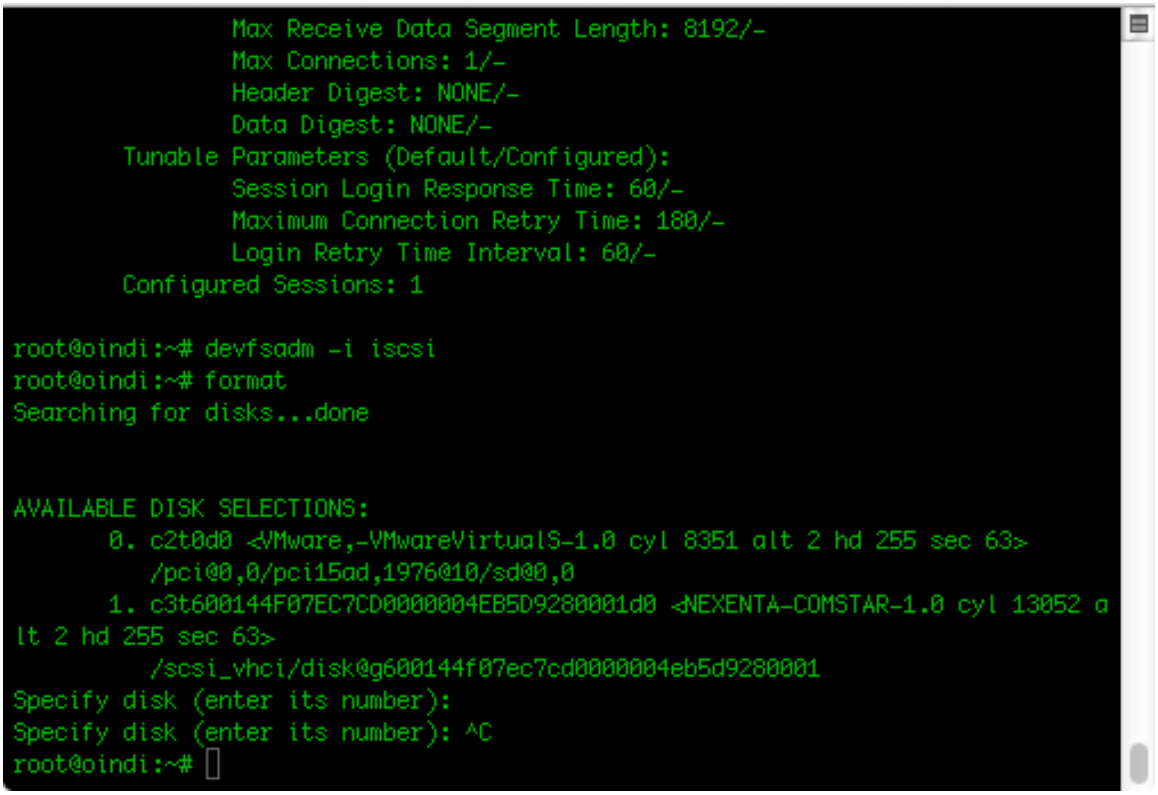

Figure 10: The command “devfsadm” can be used to scan for the device once again.

We then run format to see that the device is available for use, configured for bidirectional CHAP authentication.

Regardless of whether you choose unidirectional or bidirectional authentication you can secure your LUNs accessed using iSCSI using CHAP.