

NexentaStor

iSCSI Security Using CHAP

Nexenta Solutions Engineering Team

September 2012



Contents

Purpose	2
iSCSI Qualified Names	2
iSCSI CHAP Authentication	2
Unidirectional CHAP Implementation	
Bidirectional CHAP	



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.

→ C f (S) isan-01.techops.nex	<pre>xenta.com:2000/data/scsitarget/iscsi/tpgs/</pre>	<u> </u>
Snexenta	Support Add Capacity Register Help tatus 🔷 Settings 📀 Data Management 🄇 🗢 Analytic	Welcome Administrator Logout
🖓 V 👔 Data Sets 🛛 👔 Shares 🕺 SCSI Ta	M DataCenter 4 Irget Plus 🍓 Auto Services 👘 Runners	📕 Console 📄 View log 🌼 J
SCSI Target 🔹 🔻	MANAGE ISCSI TPGS	
<u>Mappings</u> Manage mappings. Initiator groups	Target Portal Groups [create]	[delete
Manage groups of remote initiators.	# IP Address Port	
Target groups Manage groups of local targets.	1 172.16.45.213 3260	
Zvols 🔻		
<u>View</u> View zvols.		
<u>Create</u> Create a new zvol (virtual block device).		
scsi 🔹		
<u>Remote Initiators</u> Manage iSCSI remote initiators.		
<u>Targets</u> Manage iSCSI targets.		
Target Portal Groups Manage iSCSI target portal groups.		

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"

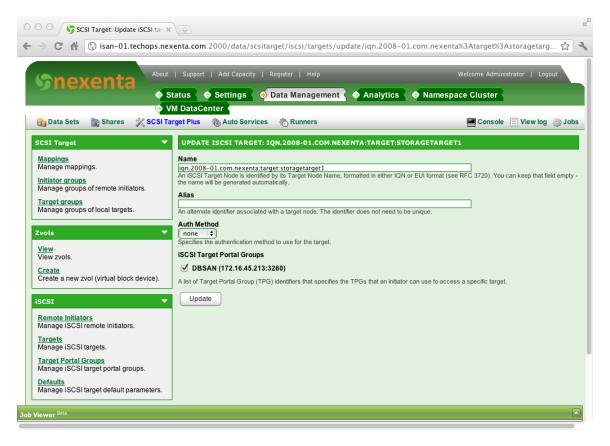


Figure 2: Leave "Auth Method" to none when creating the target.

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.

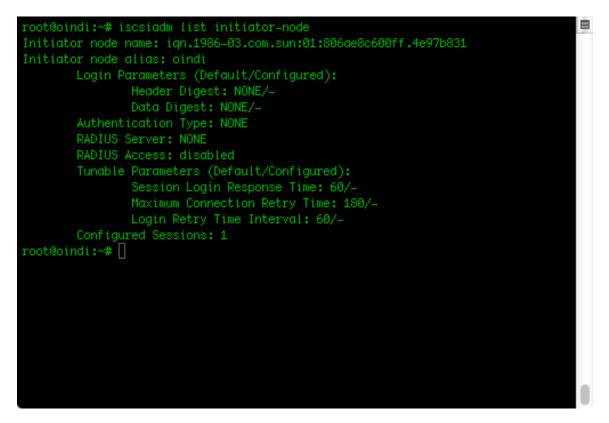


Figure 3: To acquire the IQN of the initiator, run the following command:

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).

SCSI Target: Update iSCSI ren ×		
→ C ☆ (S) isan-01.techops.nex	xenta.com:2000/data/scsitarget/iscsi/initiators/update/iqn.19	86-03.com.sun:01:806ae8c600ff.4e97b831/ 🛣
Snexenta	Support Add Capacity Register Help tatus ● Settings ● Data Management ● Analytic M DataCenter ●	Welcome Administrator Logout
😭 Data Sets 🛛 👔 Shares 💥 SCSI Ta		📕 Console 📄 View log 🌼 Jobs
SCSI Target 🔹 🔻	UPDATE ISCSI REMOTE INITIATOR: IQN.1986-03.COM.SUN:0	1:806AE8C600FF.4E97B831
Mappings Manage mappings. Initiator groups Manage groups of remote initiators. Target groups Manage groups of local targets.	initiator node name is used as the username.	e in CHAP authentication. If no value is specified then the remote ntication. There is no default for this property. Maximum length is
Zvols View View zvols,	Update	
<u>Create</u> Create a new zvol (virtual block device).		
iscsi 🗸		
Remote Initiators Manage iSCSI remote initiators.		
Targets Manage iSCSI targets.		
<u>Target Portal Groups</u> Manage iSCSI target portal groups.		
Defaults Manage iSCSI target default parameters.		
Viewer ^{Beta}	-	

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.

root@oindi:~# iscsiadm list initiator-node	
Initiator node name: iqn.1986-03.com.sun:01:806ae8c600ff.4e97b831	
Initiator node alias: oindi	
Login Parameters (Default/Configured):	
Header Digest: NONE/-	
Data Digest: NONE/-	
Authentication Type: NONE	
RADIUS Server: NONE	
RADIUS Access: disabled	
Tunable Parameters (Default/Configured):	
Session Login Response Time: 60/-	
Maximum Connection Retry Time: 180/-	
Login Retry Time Interval: 60/-	
Configured Sessions: 1	
root@oindi:~# iscsiadm modify initiator-nodeCHAP-name unclefred	
root@oindi:~# iscsiadm modify initiator-nodeCHAP-secret	
Enter secret:	
Re-enter secret:	
root@oindi:~# [

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.

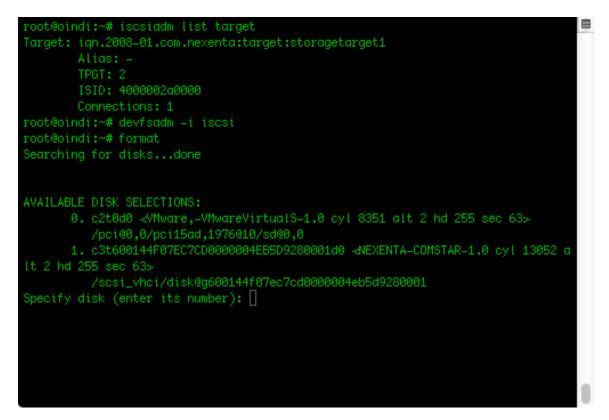


Figure 6: Finding LUNS available to the initiator using the following commands:

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



root@oindi:~# devfsadm _Cv _i iscsi Searching for disks...done AVAILABLE DISK SELECTIONS: 0. c2t0d0 </Mware,-VMwareVirtualS-1.0 cyl 8351 alt 2 hd 255 sec 63> /pci@0,0/pci15ad,1976@10/sd@0,0 1. c3t600144F07EC7CD0000004EB5D9280001d0 ⊲NEXENTA-COMSTAR-1.0 cyl 13052 a lt 2 hd 255 sec 63> /scsi_vhci/disk@g600144f07ec7cd0000004eb5d9280001 Specify disk (enter its number): ^C root@oindi:~# iscsiadm remove static-config iqn.2008-01.com.nexenta:target:stora getarget1,172.16.45.213:3260,2 root@oindi:~# devfsadm _Cv _i iscsi Searching for disks...done AVAILABLE DISK SELECTIONS: 0. c2t0d0 </Mware,-VMwareVirtualS-1.0 cyl 8351 alt 2 hd 255 sec 63> /pci@0,0/pci15ad,1976@10/sd@0,0 Specify disk (enter its number): 🛽

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.

C G isan-01.techops.ne	xenta.com:2000/data/scsitarget/iscsi/targets/update/iqn.2008-01	1.com.nexenta%3Atarget%3Astoragetarg ನ್ನ
Snexenta	Support Add Capacity Register Help status • Settings • Data Management • Analytics	Welcome Administrator Logout
🚱 🛛 資 Data Sets 🛛 👔 Shares 💥 SCSI Ta	M DataCenter 🕻 Irget Plus 🍈 Auto Services 👘 Runners	💻 Console 📄 View log 🗼 J
CSI Target 🗸 🔻	UPDATE ISCSI TARGET: IQN.2008-01.COM.NEXENTA:TARGET:STC	DRAGETARGET1
<u>Mappings</u> Manage mappings. I <u>nitiator groups</u> Manage groups of remote initiators.	Name (iqn.2008-01.com.nexenta:target:storagetarget1 An ISCSI Target Node is identified by its Target Node Name, formatted in either IQN of the name will be generated automatically.	or EUI format (see RFC 3720). You can keep that field emp
<u>Target groups</u> Manage groups of local targets.	Alias An alternate identifier associated with a target node. The identifier does not need to be	e unique.
tvols 🗸	Auth Method Chap Specifies the authentication method to use for the target.	
<u>View</u> View zvols. <u>Create</u> Create a new zvol (virtual block device).	CHAP User <u>uncleiff</u> Specifies the CHAP username for a target for use in mutual CHAP authentication. If n username.	to value is specified then the target node name is used as t
SCSI	CHAP Secret The CHAP secret to send during mutual CHAP authentication. There is no default for required length is 12 characters.	this property. Maximum length is 255 characters; minimum
Manage iSCSI remote initiators.	iSCSI Target Portal Groups	
<u>Targets</u> Manage iSCSI targets.	✓ DBSAN (172.16.45.213:3260) A list of Target Portal Group (TPG) identifiers that specifies the TPGs that an initiator	can use to access a specific target.
<u>Target Portal Groups</u> Manage iSCSI target portal groups.	Update	
Defaults		

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



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 Enter secret: Re-enter secret: root@oindi:~# iscsiadm list target_param _v iqn.2008–01.com.nexenta:target:stora getarget1 Target: iqn.2008-01.com.nexenta:target:storagetarget1 Bi-directional Authentication: disabled CHAP Name: unclejeff Login Parameters (Default/Configured): Data Sequence In Order: yes/-Data PDU In Order: yes/-Error Recovery Level: 0/-First Burst Length: 65536/-Immediate Data: yes/-Initial Ready To Transfer (R2T): yes/-Max Burst Length: 262144/-Max Outstanding R2T: 1/-

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





	_
Max Receive Data Segment Length: 8192/-	
Max Connections: 1/-	
Header Digest: NONE/-	
Data Digest: NONE/-	
Tunable Parameters (Default/Configured):	
Session Login Response Time: 60/-	
Maximum Connection Retry Time: 180/-	
Login Retry Time Interval: 60/-	
Configured Sessions: 1	
root@oindi:~# devfsadm —i iscsi	
root@oindi:~# format	
Searching for disksdone	
AVAILABLE DISK SELECTIONS:	
0. c2t0d0 ≺VMware,–VMwareVirtualS–1.0 cyl 8351 alt 2 hd 255 sec 63>	
/pci@0,0/pci15ad,1976@10/sd@0,0	
1. c3t600144F07EC7CD0000004EB5D9280001d0 ⊲NEXENTA-COMSTAR-1.0 cyl 13052 a	
It 2 hd 255 sec 63>	
/scsi_vhci/disk@g600144f07ec7cd0000004eb5d9280001	
Specify disk (enter its number):	
Specify disk (enter its number): ^C	
root@oindi:~# 🗌	

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.