



Technical Report

Element Software Microsoft Windows Configuration Guide

For SolidFire and NetApp HCI

Daniel Elder, NetApp
July 2020 | TR-4643

TABLE OF CONTENTS

1	Introduction	3
1.1	Creating a System Account	3
1.2	Creating a Volume	3
1.3	Enabling the Microsoft iSCSI Service	4
2	Access Control and Authentication for SolidFire Volumes	4
2.1	Option 1: Volume Access Groups	5
2.2	Option 2: Unidirectional CHAP	8
2.3	Option 3: Bidirectional CHAP	10
2.4	Connecting Multiple iSCSI Sessions to a Single Volume	12
2.5	Tuning MPIO Path Selection	15
2.6	Tuning TCP Failover	15
2.7	Tuning Disk and iSCSI Timeouts	16
3	Operating System Queue Depth	18
3.1	Updating the Queue Depth	18
4	Creating the Partition and Formatting the Volume	19
4.1	Prerequisites	19
4.2	Procedure	19
5	Contacting NetApp Support	20
	Where to Find Additional Information	20
	Version History	20

LIST OF TABLES

Table 1)	Queue depth recommendations	18
----------	-----------------------------	----

LIST OF FIGURES

Figure 1)	iSCSI login first path	13
Figure 2)	iSCSI login second path	14

1 Introduction

This document describes how to configure a Microsoft Windows host to connect to a NetApp® SolidFire® or NetApp HCI volume. It also provides best practices and implementation recommendations for this configuration. This guide covers configuring supported Windows Server versions. See the [Interoperability Matrix Tool \(IMT\)](#) for more details on supported configurations.

Before you can set up a connection, you must first set up an Element system account and subsequent volumes.

Note: This document assumes that you have access to the Element Software Web UI. These same procedures can be performed through the NetApp Element Plug-in for vCenter Server. For additional details, see the NetApp HCI documentation: [Using VCP to Manage NetApp HCI](#).

1.1 Creating a System Account

Each Element account represents a unique volume owner and receives its own set of Unidirectional Challenge-Handshake Authentication Protocol (CHAP) credentials. You can access volumes assigned to an account either by using the account name and its CHAP credentials or through a volume access group (VAG).

Procedure

1. Log in to the Element Software Web UI.
2. Go to Management > Accounts.
3. Click Create Account.
4. In the Username field, enter the CHAP username to be used with the Windows host.
5. In the CHAP Settings section, enter the following information:
 - The initiator secret for CHAP node session authentication
 - The target secret for CHAP node session authentication

Note: To autogenerate the secrets, leave these fields blank. To view them, click Actions > View Details.

6. Click Create Account.

1.2 Creating a Volume

After provisioning an account, you must create volumes and associate them with the account. This enables iSCSI initiators that use the provided CHAP credentials to discover and mount iSCSI devices that are associated with that account in Element OS.

Procedure

1. Go to Management > Volumes.
2. Click Create Volume.
3. In the Create a New Volume dialog box, enter the volume name (1 to 64 characters in length).
4. Enter the total size of the volume.

Note: The default volume size selection is in GB. Volumes can be created in GB or GiB:

- 1GB = 1,000,000,000bytes
- 1GiB = 1,073,741,824bytes

5. Select a block size for the volume. The NetApp recommended block size is 4K.

Note: For pre-Windows Server 2012 releases, you must select the 512-byte emulated option. For additional information on Microsoft supported block sizes, see [Microsoft KB 2510009](#).

6. Click Account and select from the list the account that should have access to the volume. If an account does not exist, click the Create Account link, enter a new account name, and click Create. The account is created and associated with the new volume.

Note: If there are more than 50 names, the list does not appear. Begin typing and the autocomplete function displays possible values for you to choose from.

Set the Quality of Service values or accept the default values.

Caution: Volumes with Max IOPS and Burst IOPS greater than 20,000 are specifically allowed to accommodate higher bandwidths. Achieving greater than 20,000 small-block IOPS on a single volume requires a high queue depth and might require special multipath I/O (MPIO) configuration.

7. Click Create Volume.

1.3 Enabling the Microsoft iSCSI Service

To connect directly to an Element volume, start the Microsoft iSCSI service. After you start the service, you have three options to authenticate your connection with the SolidFire volumes. For details about the three options, see the section “Access Control and Authentication for SolidFire Volumes.”

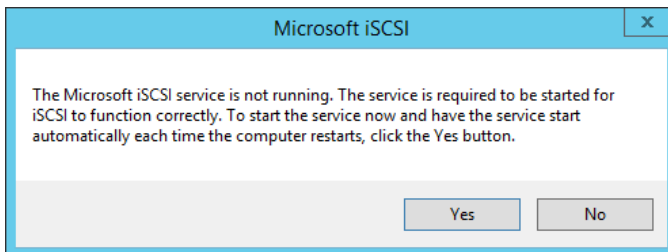
Procedure

1. Start > Control Panel > System and Security > Administrative Tools > iSCSI Initiator.

If you are using Windows Server Core, open the iSCSI Initiator tools using the `iscsicpl.exe` command.

For additional administrative command references for Windows Server Core, see [Microsoft's Server Core documentation](#).

2. Select iSCSI Initiator from the list to open the Microsoft iSCSI dialog box.



3. Click Yes to start the iSCSI service.
4. (Optional) If prompted to unblock the Microsoft iSCSI service through the Windows firewall, click Yes.

2 Access Control and Authentication for SolidFire Volumes

Access control determines which Element volumes a given iSCSI initiator can access. SolidFire offers two forms of access control to hosted volumes: accounts and VAGs:

- Account-based access control
- VAG access control

If the iSCSI initiator is configured to use CHAP authentication, account-based access control is used. If the iSCSI initiator is not configured to use CHAP authentication, VAG access control is used. You can use CHAP authentication (verification that the initiator is the intended volume user) only with account-based access control.

- **Option 1: Volume Access Groups.** VAGs provide access control between a list of iSCSI initiator IQNs and an associated group of volumes. Note that this method does not provide account name or secret authentication. Therefore, if you enter an initiator incorrectly, the host might have access to more volumes than intended. VAGs might contain volumes from more than one account.
- **Option 2: Unidirectional CHAP.** CHAP leverages an account name and one or more secrets to authenticate an initiator to a target. The use of CHAP provides for both access control (limiting access to specific volumes) and authentication (verifying that the specific initiator presents the correct credentials for access to the volume). With unidirectional CHAP, the initiator authenticates with the target.
- **Option 3: Bidirectional CHAP.** With bidirectional CHAP, the initiator authenticates with the target and the target authenticates with the initiator.

Note: This section applies only to server deployments connecting directly to an Element volume.

2.1 Option 1: Volume Access Groups

A SolidFire VAG contains a list of iSCSI qualified names (IQNs) that can access the volume without CHAP user ID and password authentication.

Finding the Initiator IQNs

You need the server initiator IQN to associate the server to the volume(s) by using a VAG.

Prerequisites

The Microsoft iSCSI service must be running.

Procedure

1. Launch the iSCSI Initiator utility to open the iSCSI Initiator Properties dialog box.
2. Click the Configuration tab.
3. Select the Initiator Name IQN and copy it for future reference.

Note: The IQN is required when Creating an Access Group or Adding Volumes to an Access Group.

Creating an Access Group

Clients can discover volumes through VAGs, which allow initiator access to volumes without requiring CHAP authentication. You can set up a VAG by using an IQN. After you create the VAG, you can assign volumes to the VAG to create a collection of volumes.

When creating an access group, note the following:

- An access group can contain a maximum of 64 initiator IQNs. Any initiator in the VAG can access any volume in the VAG.
- An IQN can belong to only one access group.
- A single volume can belong to a maximum of four access groups.

Procedure

1. Open the Element Web UI.
2. Go to Management > Access Groups.
3. Click Create Access Group.
4. Enter a name for the VAG in the Name field.

- To add an iSCSI initiator to the VAG, under Add Initiators, select an existing initiator from the Initiators list.

Note: You can create an initiator during this step by clicking the Create Initiator link, entering an initiator name, and clicking Create. The system automatically adds the initiator to the Initiators list when you create it.

The accepted format of an initiator IQN is `iqn.yyyy-mm`, where `y` and `m` are digits, followed by text which must only contain digits, lowercase alphabetic characters, periods (`.`), colons (`:`), or dashes (`-`).

Example:

```
iqn.1991-05.com.microsoft:servername
```



TIP: You can find the initiator IQN for each volume by selecting View Details in the Actions menu for the volume on the Management > Volumes > Active list.

- (Optional) Add more initiators as needed.
- Under Attach Volumes, select a volume from the Volumes list.
The volume appears in the Attached Volumes list.
- (Optional) Add more volumes as needed.
- Click Create Access Group.

Adding Initiators to an Access Group

You can add an initiator to an Access Group to allow access to volumes in the VAG without requiring CHAP authentication. When you add an initiator to a VAG, the initiator has access to all volumes in that VAG.

Procedure

- Go to Management > Access Groups.
- Click the Actions button () for the access group that you want to edit.
- Click the Edit button ().
- To add an iSCSI initiator to the VAG, complete the following steps:
 - Under Add Initiators, select an existing initiator from the Initiators list.
 - Click Add Initiator.

Note: You can create an initiator during this step by clicking the Create Initiator link, entering an initiator name, and clicking Create. The system automatically adds the initiator to the Initiators list after you create it.

TIP: You can find the initiator IQN for each volume by selecting View Details in the Actions menu for the volume on the Management > Volumes > Active list.

- (Optional) Repeat step 4 to add more initiators as needed.
- Click Save Changes.

Adding Volumes to an Access Group

You can add volumes to a VAG. Volumes can belong to more than one VAG, and you can see the groups that each volume belongs to in the Active Volumes window.

Note: You can also follow these steps to add volumes to a Fibre Channel VAG.

Procedure

- Go to Management > Access Groups.

2. Choose an access group and click the Actions button (⚙️).
3. In the resulting menu, click the Edit button (✎️).
4. Under Add Volumes, select a volume from the Volumes list.
5. Click Attach Volume.
6. Repeat steps 5 and 6 to add more volumes as needed.
7. Click Save Changes.

Discovering and Logging into the iSCSI Volume

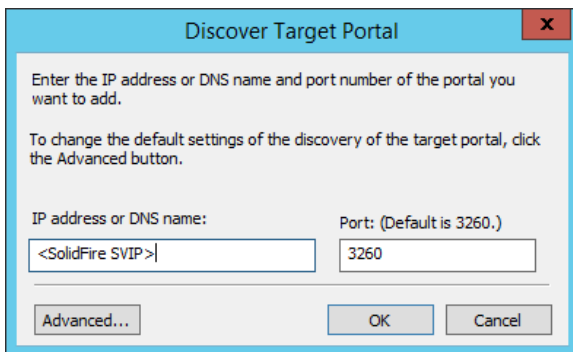
This section details the steps to discover the Element volumes and log in to them using a single iSCSI session.

Prerequisites

- The Microsoft iSCSI service is installed and running.
- You have added at least one volume to the configured account or VAG.
- You have configured authentication through VAGs, unidirectional CHAP, or bidirectional CHAP.

Procedure

1. Launch the iSCSI Initiator utility to open the iSCSI Initiator Properties dialog box.
2. Click the Discovery tab.
3. Click Discover Portal to open the Discover Target Portal dialog box.



4. In the IP Address or DNS Name field, enter the IP address of the Storage Virtual IP (SVIP).
5. Click OK.
6. Click the Targets tab and verify that the volume has been discovered or added correctly and is listed in the targets list.

Note: The volume name is included in the target IQN. In this example, the volume name is `newvolume-0`.

7. Click Connect to open the Log On to Target or Connect to Target dialog box.
8. (Optional) If you want the volume to automatically log in at boot up, select Add This Connection to the List of Favorite Targets check box to select it.
9. (Optional) If the volume is used for a high-performance application, see the section “Connecting Multiple iSCSI Sessions to a Single Volume” for details about configuring MPIO.
10. Click OK.

The status shows Connected.

11. Go to the section “Operating System Queue Depth” for the next steps.

2.2 Option 2: Unidirectional CHAP

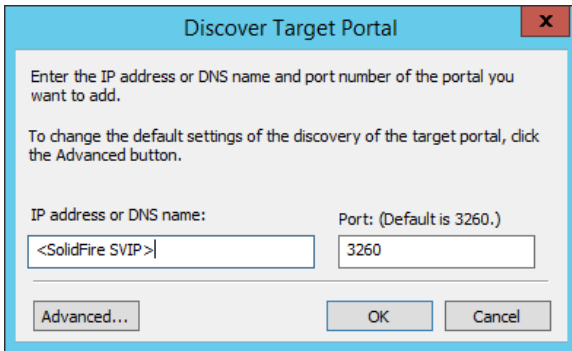
The unidirectional CHAP option authenticates volume access by using the Element account name and initiator secret.

Prerequisites

- The Microsoft iSCSI service must be installed and running.
- Make sure that there is an existing Element account and associated volumes.

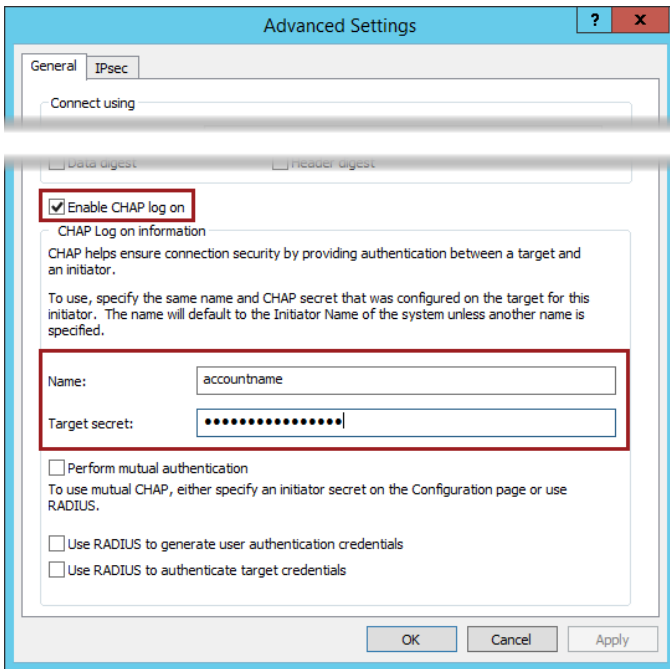
Procedure

1. Launch the iSCSI Initiator utility to open the iSCSI Initiator Properties dialog box.
2. Click the Discovery tab.
3. Click Discover Portal to open the Discover Target Portal dialog box.



The Discover Target Portal dialog box has a title bar with a close button (X). The main area contains the following text: "Enter the IP address or DNS name and port number of the portal you want to add." and "To change the default settings of the discovery of the target portal, click the Advanced button." Below this, there are two input fields: "IP address or DNS name:" with the text "<SolidFire SVIP>" and "Port: (Default is 3260.)" with the value "3260". At the bottom, there are three buttons: "Advanced...", "OK", and "Cancel".

4. In the IP Address or DNS Name field, enter the IP address of the SVIP.
5. Click Advanced to open the Advanced Settings dialog box.



The Advanced Settings dialog box has a title bar with a help button (?) and a close button (X). It has two tabs: "General" and "IPsec". The "IPsec" tab is selected. Below the tabs, there is a "Connect using" dropdown menu. Below that, there are two checkboxes: "Data digest" and "Header digest", both of which are unchecked. The "Enable CHAP log on" checkbox is checked and highlighted with a red box. Below this, there is a section titled "CHAP Log on information" with the text: "CHAP helps ensure connection security by providing authentication between a target and an initiator. To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified." Below this text, there are two input fields: "Name:" with the text "accountname" and "Target secret:" with a masked password ".....". These two fields are also highlighted with a red box. At the bottom, there are three buttons: "OK", "Cancel", and "Apply".

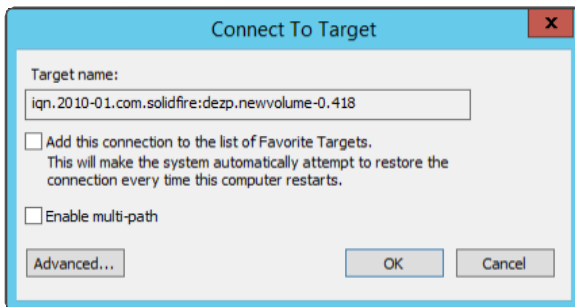
6. Click the Enable CHAP Log On check box to select it.
7. Enter the username (Element system account name) and target secret (Element initiator secret).

Note: The Windows user interface refers to secrets differently than Element. During iSCSI configuration, use the Element initiator secret anywhere that the Windows user interface requests a target secret, and use the Windows initiator secret anywhere the Element user interface requests a target secret.

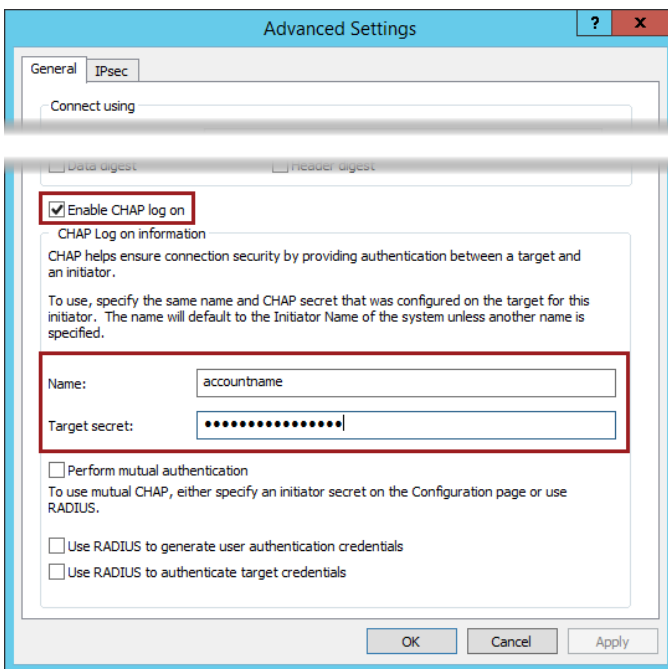
8. Click OK.
9. Click OK again.
10. Click the Targets tab and verify that the volume has been discovered or added correctly and is listed in the target list.

Note: The volume name is included in the target IQN. In this example, the volume name is `newvolume-0`.

11. Click Connect to open the Log On to Target or Connect to Target dialog box.



12. Click Advanced to open the Advanced Settings dialog box.



13. Click the Enable CHAP Log On check box to select it.
14. Enter the username (Element system account name) and target secret (Element initiator secret).

Note: The Windows user interface refers to the secrets differently than Element. During iSCSI configuration, use the Element initiator secret anywhere that the Windows user interface requests a target secret, and use the Windows initiator secret anywhere the Element user interface requests a target secret.

15. Click OK.
16. (Optional) If you want the volume to automatically log in at boot up, click the Add This Connection to the List of Favorite Targets check box to select it.
17. (Optional) If the volume is to be used for a high-performance application, see the section “Connecting Multiple iSCSI Sessions to a Single Volume” for details about configuring MPIO.
18. Click OK.
The status shows Connected.
19. Go to the section “Operating System Queue Depth” for the next steps.

2.3 Option 3: Bidirectional CHAP

The bidirectional CHAP option provides the most secure way of authenticating the volume, but it also requires the most configuration. With this method, the volume authenticates the host through the account name and the initiator secret, and then the host authenticates the volume through the account name and the target secret.

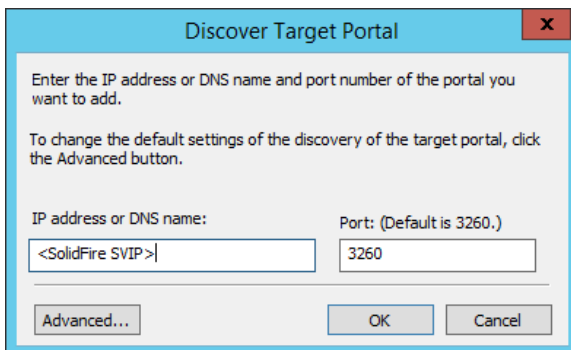
Note: For the best security, the initiator secret and target secret should be different.

Prerequisites

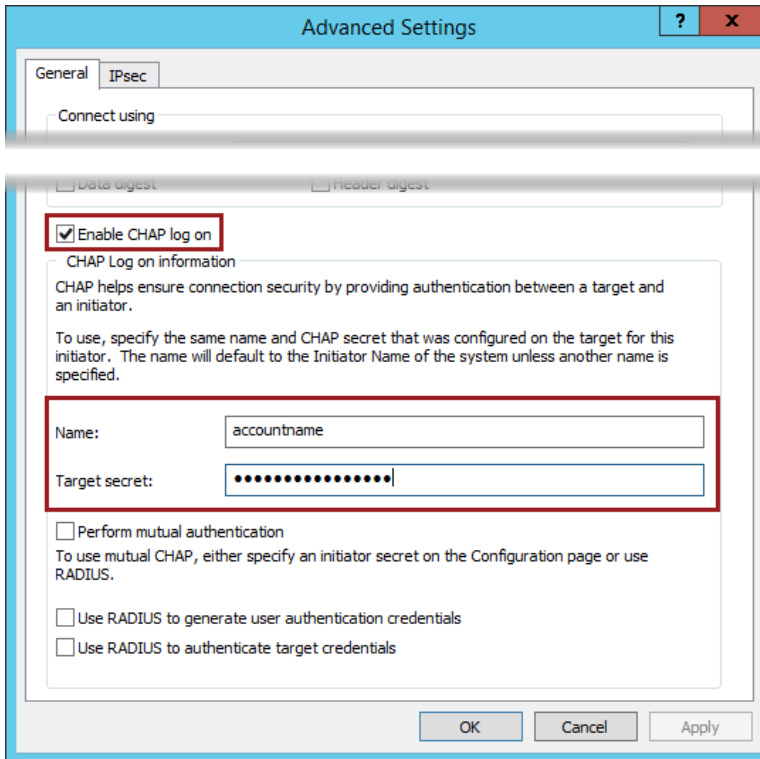
- The Microsoft iSCSI service must be installed and running.
- Verify that there is an existing Element account and associated volumes.

Procedure

1. Launch the iSCSI Initiator utility to open the iSCSI Initiator Properties dialog box.
2. Click the Configuration tab.
3. Click CHAP for mutual CHAP authentication.
4. Enter the SolidFire target secret.
5. Click OK.
6. Click the Discovery tab.
7. Click Discover Portal to open the Discover Target Portal dialog box.



8. In the IP Address or DNS Name field, enter the IP address of the SVIP.
9. Click Advanced to open the Advanced Settings dialog box.



10. Click the Enable CHAP Log On check box to select it.

11. Enter the username (Element system account name) and target secret (Element initiator secret).

Note: The Windows user interface refers to the secrets differently than Element. During iSCSI configuration, use the Element initiator secret anywhere that the Windows user interface requests a target secret, and use the Windows initiator secret anywhere the Element user interface requests a target secret.

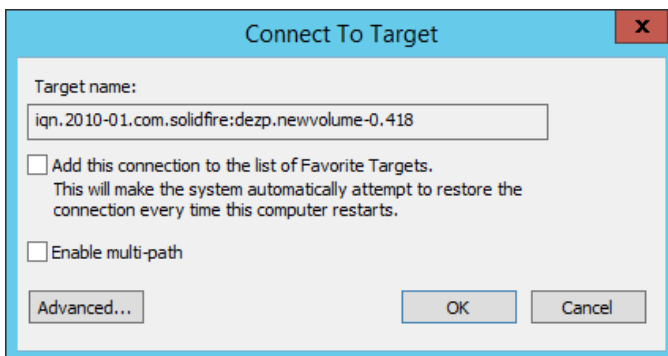
12. Click OK.

13. Click OK again.

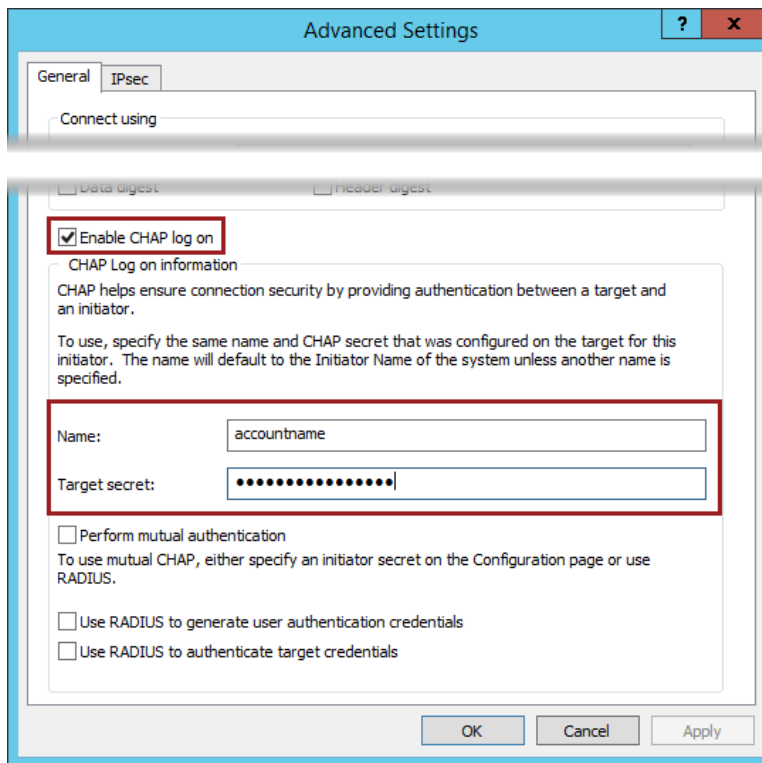
14. Click the Targets tab and verify that the volume has been discovered or added correctly and is listed in the targets list.

Note: The volume name is included in the target IQN. In this example, the volume name is `newvolume-0`.

15. Click Connect to open the Log On to Target or Connect to Target dialog box.



16. Click Advanced to open the Advanced Settings dialog box.



17. Click the Enable CHAP Log On check box to select it.

18. Enter the username (Element system account name) and target secret (Element initiator secret).

Note: The Windows user interface refers to the secrets differently than Element. During iSCSI configuration, use the Element initiator secret anywhere that the Windows user interface requests a target secret, and the Windows initiator secret anywhere the Element user interface requests a target secret.

19. Click the Perform Mutual Authentication check box to select it.

20. Click OK.

21. (Optional) If you want the volume to automatically log in at boot up, click the Add This Connection to the List of Favorite Targets check box to select it.

22. (Optional) If the volume is to be used for a high-performance application, see the section “Connecting Multiple iSCSI Sessions to a Single Volume,” for details about configuring MPIO.

23. Click OK.

The status shows Connected.

24. Go to the section “Operating System Queue Depth” for the next steps.

2.4 Connecting Multiple iSCSI Sessions to a Single Volume

This section details the steps to connect multiple iSCSI sessions to a single Element iSCSI volume. Multiple iSCSI sessions are useful in two scenarios. One, you might want to leverage two physical network interface controllers (NICs) for your iSCSI traffic. Two, you might want to increase the aggregate queue depth to a single volume.

Prerequisite

Verify that you have access to a Microsoft Windows server with multiple physical or virtual NICs on the appropriate storage network.

Procedure

This example uses Windows Server 2012 R2 Datacenter with four 10GB virtual NICs.

1. Install MPIO:
 - a. Select Start > Control Panel > System and Security > Administrative Tools.
 - b. Double-click Server Manager.
 - c. In the Features area, click Add Features to open the Add Features Wizard.
 - d. Click the Multipath I/O check box to select it.
 - e. Click Next to open a confirmation dialog box.
 - f. Click Install.
 - g. When the installation is complete, click Close.

Note: A reboot might be required, depending on your version of Windows Server.

 - h. (Optional) If prompted to restart the computer, click Yes.
 - i. (Optional) After the computer reboots and finalizes the MPIO installation, click Close.
2. Start Microsoft iSCSI Initiator:
 - a. Click Start > Control Panel > System and Security > Administrative Tools.
 - b. Double-click iSCSI Initiator to open the Microsoft iSCSI dialog box.
 - c. (Optional) If a Microsoft iSCSI dialog box opens asking to start the service, click Yes.
 - d. Click the Discovery tab.
 - e. Click Discover Portal.
 - f. In the IP Address or DNS Name field, enter the IP address of the SVIP.
 - g. Click Advanced to open the Advanced Settings dialog box.
 - h. On the General tab, verify that the source IP/initiator IP is set to default so that discovery of the LUN occurs through all the paths.
 - i. (Optional) If using CHAP credentials, click the Enable CHAP Log On check box and enter the account name and secret.
 - j. Click OK twice.
 - k. Click the Targets tab.
 - l. Click Connect.
 - m. Click the top check box to automatically log into the volume at boot up.

Note: Each path requires a separate login:

Figure 1) iSCSI login first path.

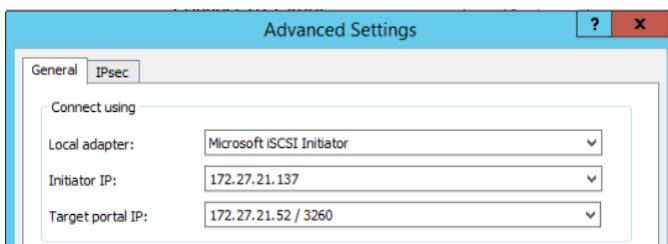
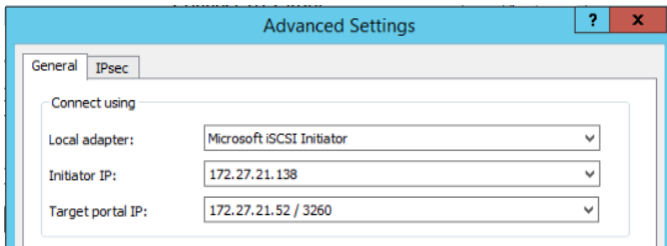
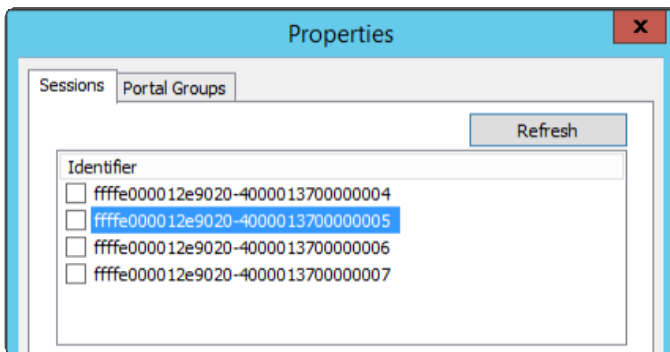


Figure 2) iSCSI login second path.



- n. Click the Enable Multi-Path check box to select it.
- o. Continue to log in to all the remaining paths, using all available initiator IP addresses if your server has more than one. For example, session 1 and session 3 use IP #1, and session 2 and session 4 use IP #2.
- p. When all paths have an iSCSI connection, select the target and click Properties to open the Properties dialog box.

The number of identifiers equals the number of desired paths when the multipath iSCSI sessions have been created correctly.



- q. Click OK.
3. Combine multiple sessions into a single disk:
 - a. Click Start > Control Panel > System and Security > Administrative Tools.
 - b. Double-click MPIO.
 - c. Click the Discover Multi-Path tab.
 - d. Select Add Support for iSCSI devices.
 - e. Click Add.

A reboot might be required, depending on your version of Windows Server.

- f. Navigate back to the Administrative Tools window and double-click iSCSI Initiator.
- g. Click the Targets tab.
- h. Click Details.
- i. Click Devices.
- j. Click MPIO.
- k. Set the load balancing policy to Least Queue Depth.
The disk can now be formatted for use through disk management.
- l. To verify that multipath is using all paths correctly, run a high queue-depth workload and see that SolidFire is receiving a queue depth of more than 16.

2.5 Tuning MPIO Path Selection

By default, Microsoft Windows MPIO uses a round-robin policy for spreading load across all connected paths to a volume. In SolidFire lab testing, changing the MPIO policy to Least Queue Depth provided the best performance during path failure scenarios.

Procedure

1. Open Computer Management (`compmgmt.msc`).
2. Expand Storage in the left panel.
3. Click Disk Management and wait for the view to refresh.
4. Right-click the disk you would like to modify (for example, Disk 3).
5. Select the MPIO tab.
6. In the Select the MPIO Policy menu, select Least Queue Depth.
7. Click OK to apply the changes.

2.6 Tuning TCP Failover

By default, the failover from a failed NIC to an active NIC on Microsoft Windows can take as long as 30 seconds. The following process decreases the failover time to 1 second.

Note: This process requires editing the Microsoft Windows registry. NetApp strongly recommends that you back up the registry before changing these settings and document the initial key values in case you need to revert back.

Note: HKEY_LOCAL_MACHINE is abbreviated as HKLM in some of the following descriptions.

Procedure

1. Open the Microsoft Windows Registry Editor (`regedit.exe`).
2. Edit or create the following entries:

Entry	Description
Entry	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions
Action	Create as a REG_DWORD and set value to 1.
Default	5, but registry entry does not exist
Reference	http://technet.microsoft.com/en-us/library/cc938210.aspx
Entry	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectRetransmissions
Action	Create as a REG_DWORD and set value to 1
Default	2, but registry entry does not exist
Reference	http://technet.microsoft.com/en-us/library/cc938209.aspx
Entry	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TCPInitialRtt
Action	Create as a REG_DWORD and set value to 1

Entry	Description
Default	3, but registry entry does not exist
Reference	http://technet.microsoft.com/en-us/library/cc938207.aspx

3. Reboot the server for the settings to take effect.
4. Verify the settings by running a sample load to the connected volume and disabling one of the connections—that is, pulling a cable, disabling a switch port, or disabling a vNIC.

2.7 Tuning Disk and iSCSI Timeouts

By default, Microsoft Windows disk timeouts are tuned for directly connected, local disks. For SAN volumes, you can tune some of the parameters for optimal performance. The following changes improve the performance of your SolidFire volumes during failover and volume migration. If you are using a database, including SQL Server, NetApp recommends tuning the iSCSI timeout values to avoid any connection errors in the event of a SolidFire node failure. See the NetApp Best Practices Guide for the database you are using.

This process requires editing the Microsoft Windows registry. NetApp strongly recommends that you back up the registry before changing these settings and document initial key values in case you need to revert back. In some cases, the specified registry keys might not exist by default. In those cases, create a new REG_DWORD entry with the specified name and decimal value.

Procedure

1. Open the Microsoft Windows Registry Editor (`regedit.exe`).
2. If any of the following entries do not already exist, create them as a REG_DWORD.
3. Set each of the following entries:

Entry	Description
Entry	HKLM\SYSTEM\CurrentControlSet\Services\Disk\TimeoutValue
Action	Set value to 60 (decimal) default
Default	Varies
Entry	HKLM\System\CurrentControlSet\Services\mpio\Parameters\PDORemovePeriod
Action	Set value to 120 (decimal)
Default	25
Entry	HKLM\System\CurrentControlSet\Services\mpio\Parameters\UseCustomPathRecoveryInterval
Action	Set value to 1
Default	0
Entry	HKLM\System\CurrentControlSet\Services\mpio\Parameters\PathRecoveryInterval
Action	Set value to 60 (decimal)
Default	Varies

Entry	Description
Entry	HKLM\System\CurrentControlSet\Services\mpio\Parameters\PathVerifyEnabled
Action	Set value to 1
Default	0
Entry	HKLM\System\CurrentControlSet\Services\mpio\Parameters\PathVerificationPeriod
Action	Set value to 30 (decimal)
Default	30

iSCSI Values

Entry	Description
Entry	HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\<Instance ID>\Parameters\MaxRequestHoldTime
Action	Set value to 90 (decimal)
Default	60
Notes	<Instance ID> can be identified by looking for the instance (0000, 0002, and so on) that has the parameters key beneath it. The other IDs do not have this key.
Entry	HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\<Instance ID>\Parameters\WMIRequestTimeout
Action	Set value to 120 (decimal)
Default	30
Notes	<Instance ID> can be identified by looking for the instance (0000, 0002, and so on) that has the parameters key beneath it. The other IDs do not have this key.
Entry	HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\<Instance ID>\Parameters\LinkDownTime
Action	Set value to 120 (decimal)
Default	15
Notes	<Instance ID> can be identified by looking for the instance (0000, 0002, and so on) that has the parameters key beneath it. The other IDs do not have this key.
Entry	HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\<Instance ID>\Parameters\EnableNOPOut
Action	Set value to 1
Default	0
Notes	<Instance ID> can be identified by looking for the instance (0000, 0002, and so on) that has the parameters key beneath it. The other IDs do not have this key.

3 Operating System Queue Depth

To optimize Quality of Service (QoS), you must update the volume queue depth to the appropriate value. If the queue depth is set too high, then frames remain in the active queue for too long. If the queue depth is set too low, then the volume is unable to reach its optimal performance levels.

Table 1 helps you to evaluate what your queue depth should be.

Table 1) Queue depth recommendations.

Minimum IOPS	Queue Depth
100–199	1
200–399	2
400–799	4
800–1599	8
1600–3199	16
3200–6399	32
6400+	64*

*A single Element iSCSI session supports a queue depth of 32. If a higher queue depth is required, multiple iSCSI sessions should be used in combination with MPIO.

In addition, certain hypervisors and HBAs might throttle queue depth. See the Technical Report regarding [NetApp SolidFire Quality of Service \(QoS\)](#) for additional details.

Note: The queue depth settings listed are suggestions only. They should be used as a starting point for tuning your OS and application performance.

3.1 Updating the Queue Depth

This section explains how to change the queue depth on a specific device by using the regedit tool. Verify the default queue depth prior to changing in the event a revert is necessary.

Procedure

1. Click the Start button.
2. In the Search Programs and Files field, enter `regedit`.
3. Press Enter.
4. Click Yes to open the Registry Editor.
5. Navigate to the following adapters and do the following for each:

Note: Depending on the adapter type, `ql3200`, `elxstor`, or `pviscsi` might be slightly different. If the Parameters folder or the Device folder does not exist, create them.

- **Qlogic.** HKEY_LOCAL_MACHINE > SYSTEM > CurrentControllerSet > Services > ql3200 > Parameters > Device
- **Emulex.** HKEY_LOCAL_MACHINE > SYSTEM > CurrentControllerSet > Services > elxstor > Parameters > Device
- **ParaVirtual.** HKEY_LOCAL_MACHINE > SYSTEM > CurrentControllerSet > Services > pviscsi > Parameters > Device
 - a. Create a new string value named DriverParameter.

- b. Modify the DriverParameter of the string value and set it to `qd=#`, where # is the queue depth value desired.

Note: If there is already an entry in the DriverParameter, add `qd=#` with a semicolon separating them.

4 Creating the Partition and Formatting the Volume

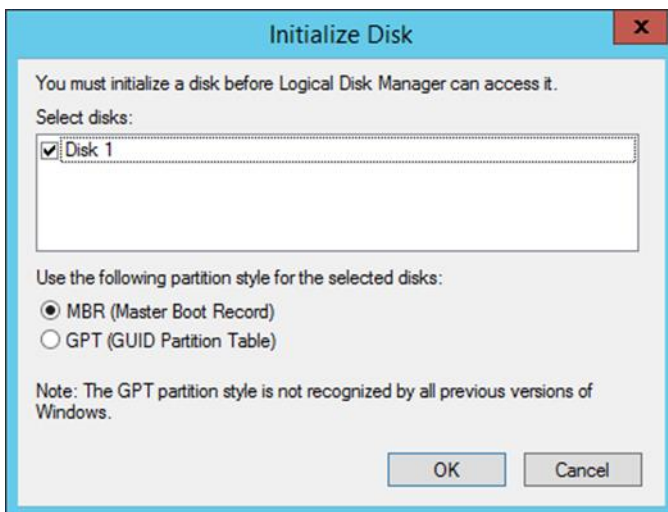
You must configure iSCSI volumes connected to Microsoft Windows servers as online, initialized, and formatted to use them for file-system storage. The detailed steps follow. Depending on your intended use for this iSCSI volume, the steps might vary slightly. See your application documentation for details.

4.1 Prerequisites

Verify that you have connected iSCSI volumes.

4.2 Procedure

1. Initialize the disk:
 - a. Click Start > Control Panel > System and Security > Administrative Tools > Computer Management to open the Computer Management window.
 - b. In the left pane, expand Storage and click Disk Management.
 - c. In the bottom right of the window, navigate to the newly added disk.
 - d. Right-click the disk and select Online from the menu.
 - e. Right-click the disk again and select Initialize Disk from the menu to open the Initialize Disk confirmation dialog box.



- f. Select MBR or GPT. NetApp recommends using the GPT partition style. For partitioned space less than 2TiB that uses the 512-byte emulated block size, MBR can still be used. For more information, See Microsoft's [Windows and GPT FAQ](#).
 - g. Click OK.
 - h. Right-click the unallocated volume and select New Simple Volume from the menu to open the New Simple Volume Wizard.
2. Click Next.
3. Specify the volume size and click Next.

4. Assign a drive letter for the volume drive path and click Next to open the Format Partition dialog box.
5. Select Format This Volume with the following settings and choose these options:
 - File system = NTFS
 - Allocation unit size = Default
6. Enter a name for the volume in the Volume Label field.
7. Select the Perform a Quick Format check box.
8. Click Next.
9. Click Finish.

5 Contacting NetApp Support

If you have any questions or comments about Element and NetApp HCI documents or products in general, contact NetApp support at +1-888-4-NETAPP or email support@netapp.com.

Where to Find Additional Information

To learn more about the information in this document, refer to the following documents and/or websites:

- NetApp Support
<https://mysupport.netapp.com>
- NetApp SolidFire Resources
<https://www.netapp.com/us/documentation/solidfire.aspx>
- NetApp HCI Resources
<https://www.netapp.com/us/documentation/hci.aspx>

Version History

Version	Date	Document Version History
Version 1.0	October 2017	Initial release.
Version 1.1	July 2020	Updates for terminology, software releases, and best practices. Corrections for clarity.

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TR-4643-1017