Technical Report

NetApp SolidFire Storage for Microsoft Windows Configuration Guide

For Element OS Version 9.1

The NetApp SolidFire Engineering Team, NetApp

October 2017 | TR-4643

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This document describes how to configure a Microsoft Windows host to connect to a NetApp® SolidFire® volume. It also provides best practices and implementation recommendations for this configuration. This guide covers Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. The configuration steps are the same for each operating system version.

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

Note: This document assumes that you have access to the NetApp SolidFire Element® OS Web UI.

1.1 Creating a SolidFire Account

Each SolidFire 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.

Procedure

1. Log in to the Element OS 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 SolidFire 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. In the case of volumes that are connected with Fibre Channel (FC), the account serves as a container for the volumes, providing individual account statistics and segmentation.

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.

This option is necessary to support operating systems and applications that do not recognize native 4K drives, such as VMware ESXi.

Versions of Microsoft Windows earlier than Windows Server 2012 and Windows 8 can operate only on a native 512-byte logical block size. For compatibility with the array, you must enable 512-byte emulation. If a volume is not 512-byte emulated, Windows might not allow the volume to be discovered, partitioned, or formatted. For additional information, consult the Partition Alignment Configuration Guide on the NetApp Support site.

For Windows Server 2012 and Windows 8, NetApp still recommends that you use a volume with 512-byte emulation enabled for possible backward compatibility.

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.

7. Set the Quality of Service values or accept the default values. Use the spin box in each column to select the desired IOPS 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.

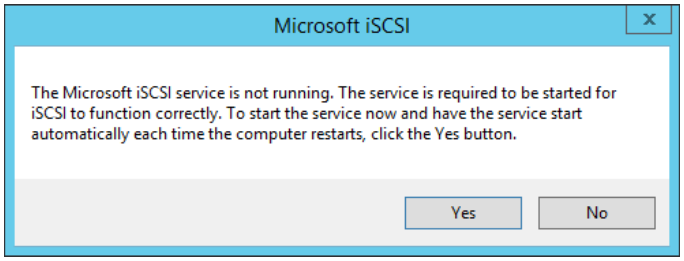
8. Click Create Volume.

1.3 Enabling the Microsoft iSCSI Service

To connect directly to a SolidFire 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. Click Start > Control Panel > System and Security > Administrative Tools.
2. Select iSCSI Initiator from the list to open the Microsoft iSCSI dialog box.



The Microsoft iSCSI service is not running. The service is required to be started for iSCSI to function correctly. To start the service now and have the service start automatically each time the computer restarts, click the Yes button.

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 SolidFire volumes a given iSCSI initiator can access. SolidFire offers two forms of access control to hosted volumes: accounts and volume access groups:

- Account-based access control
- volume access group 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, volume access group 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.** Volume access groups provide access control between a list of iSCSI initiator IQNs or FC WWPNs 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. Volume access groups might contain volumes from more than one account.
- **Option 2: Unidirectional CHAP.** CHAP is a protocol that 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 a SolidFire volume. For virtual servers, see the guide *Configuring VMware vSphere for Element* OS for connecting through a hypervisor layer.

2.1 Option 1: Volume Access Groups

A SolidFire volume access group contains a list of iSCSI qualified names (IQNs) or Fibre Channel WWPNs 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 SolidFire volume access group.

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.

Finding the Initiator WWPNs

You need the server initiator WWPN to associate the server to the volume(s) by using a SolidFire volume access group.

Procedure

There are a number of methods for determining the WWPNs of an HBA on a Windows host. Here are two methods that our lab testing has confirmed to work:

Install the Microsoft fcinfo.exe Tool

1. Download the `fcinfo.exe` tool from the following link:

https://www.microsoft.com/en-us/download/details.aspx?id=17530

2. Install the tool by following the normal installation path.
3. Run the tool from a command or PowerShell window:

```
C:\Windows\System32\fcinfo.exe /details
```

Using PowerShell and WMI Cmdlets

1. Open a PowerShell window.
2. Run the following PowerShell script to display the WWPNs:

```
Get-WmiObject -class  MSFC_FCAdapterHBAAttributes -namespace "root\WMI" | ForEach-Object
{(($_.NodeWWN) | ForEach-Object {"{0:x2}" -f $_}) -join ":"}
```

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

Creating an Access Group

Clients can discover volumes through volume access groups, which allow initiator access to volumes without requiring CHAP authentication. You can set up a volume access group by using an IQN or WWPN. After you create the volume access group, you can assign volumes to the volume access group 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 or WWPNs. Any initiator in the volume access group can access any volume in the volume access group.
- An IQN or WWPN can belong to only one access group.
- A single volume can belong to a maximum of four access groups.

Procedure

1. Open the SolidFire Element OS Web UI.
2. Go to Management > Access Groups.
3. Click Create Access Group.
4. Enter a name for the volume access group in the Name field.
5. To add a Fibre Channel initiator to the volume access group, complete the following steps:
    a. Under Add Initiators, select an existing Fibre Channel initiator from the Unbound Fibre Channel Initiators list.
    b. Click Add FC Initiator.

    Note: SolidFire systems display only WWPNs that are properly zoned and visible on the Fibre Channel network and that have not been previously added to another volume access group.
6. To add an iSCSI initiator to the volume access group, 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.

7. (Optional) Add more initiators as needed.
8. Under Attach Volumes, select a volume from the Volumes list.

   The volume appears in the Attached Volumes list.
9. (Optional) Add more volumes as needed.
10. 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 volume access group without requiring CHAP authentication. When you add an initiator to a volume access group, the initiator has access to all volumes in that volume access group.

Procedure

1. Go to Management > Access Groups.
2. Click the Actions button (⚙) for the access group that you want to edit.
3. Click the Edit button (✏).
4. To add a Fibre Channel initiator to the volume access group, complete the following steps:
   a. Under Add Initiators, select an existing Fibre Channel initiator from the Unbound Fibre Channel Initiators list.
   b. Click Add FC Initiator.
5. To add an iSCSI initiator to the volume access group, complete the following steps:
   a. Under Add Initiators, select an existing initiator from the Initiators list.
   b. 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.
6. (Optional) Repeat steps 4 and 5 to add more initiators as needed.
7. Click Save Changes.

Adding Volumes to an Access Group

You can add volumes to a volume access group. Volumes can belong to more than one volume access group, 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 volume access group.

Procedure

1. 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

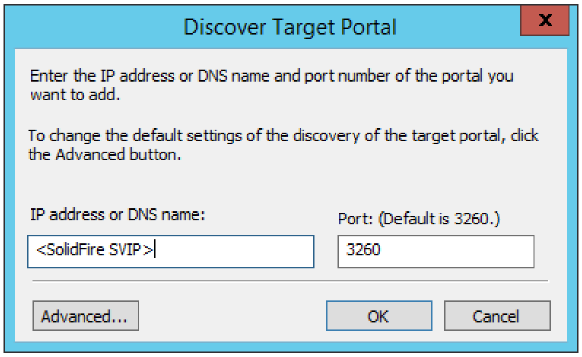
This section details the steps to discover the SolidFire volumes and log in to them using a single iSCSI session.

Prerequisites

- The Microsoft iSCSI service is installed and running.
- You have added at least one volume to the configured account or volume access group.
- You have configured authentication through volume access groups, 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.



Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: <SolidFire SVIP>

Port: (Default is 3260.) 3260

4. In the IP Address or DNS Name field, enter the IP address of the SolidFire 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

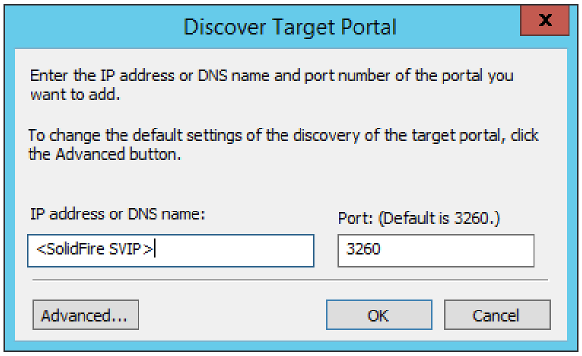
The unidirectional CHAP option authenticates volume access by using the SolidFire account name and initiator secret.

Prerequisites

- The Microsoft iSCSI service must be installed and running.
- Make sure that there is an existing SolidFire 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.



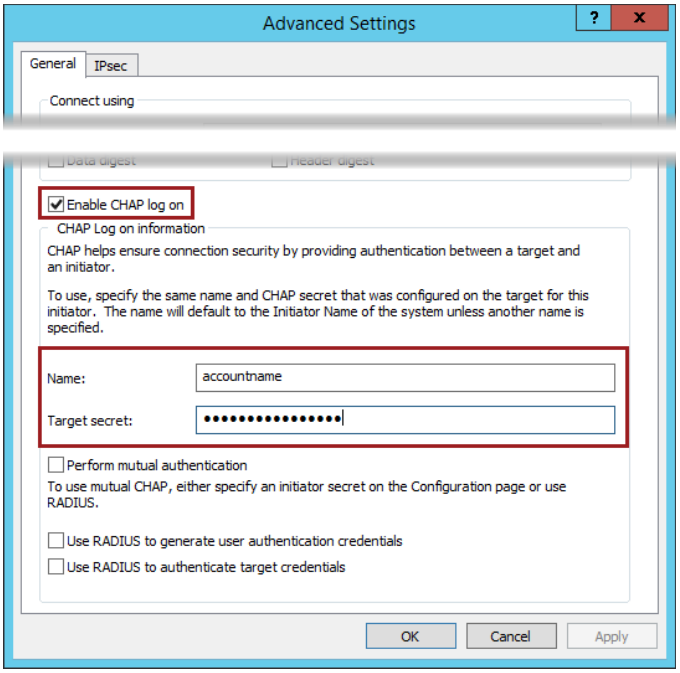
Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: <SolidFire SVIP>

Port: (Default is 3260.) 3260

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.



☑ Enable CHAP log on

CHAP Log on information

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.

Name: accountname

Target secret: ••••••••••••••••

☐ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

☐ Use RADIUS to generate user authentication credentials

☐ Use RADIUS to authenticate target credentials

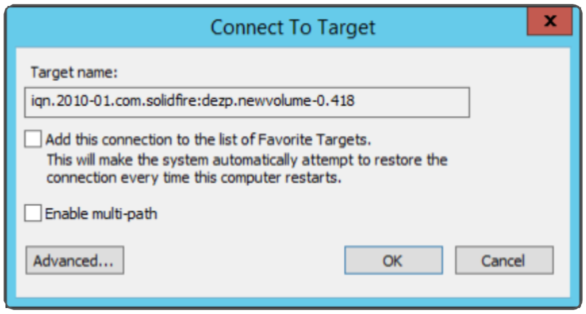
6. Click the Enable CHAP Log On check box to select it.
7. Enter the user name (SolidFire account name) and target secret (SolidFire initiator secret).

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



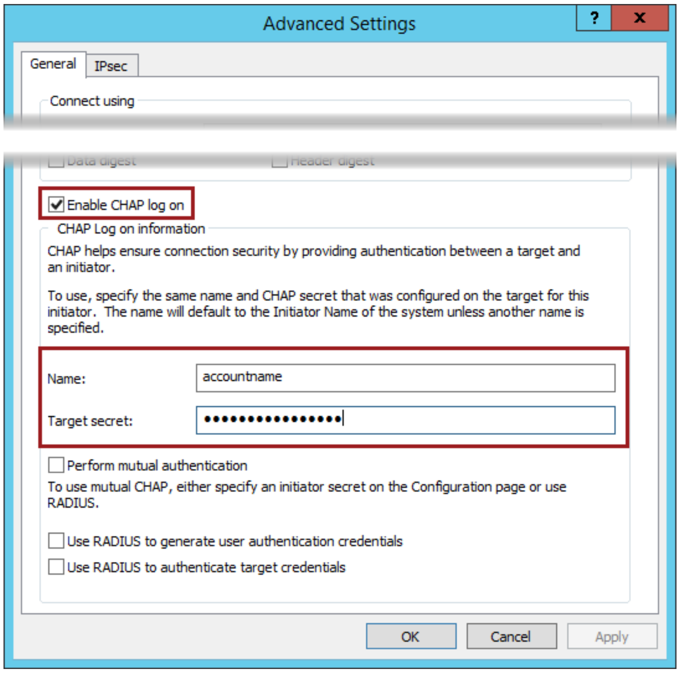
Connect To Target

Target name:
iqn.2010-01.com.solidfire:dezp.newvolume-0.418

□ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

□ Enable multi-path

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



Advanced Settings

General | IPsec

Connect using

□ Data digest □ Header digest

☑ Enable CHAP log on

CHAP Log on information

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.

Name: accountname

Target secret: ••••••••••••••••

□ Perform mutual authentication
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials
□ Use RADIUS to authenticate target credentials

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

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

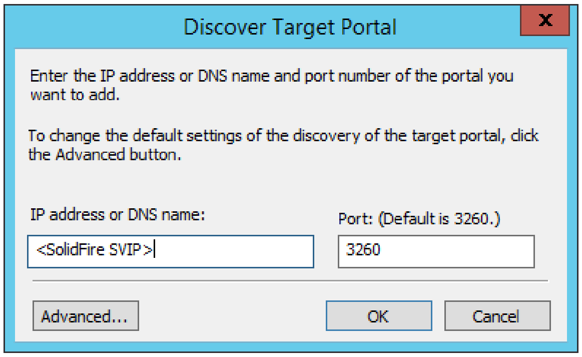
Note: For the best security, the initiator secret and target secret should be different.

Prerequisites

- The Microsoft iSCSI service must be installed and running.
- Verify that there is an existing SolidFire 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.



Discover Target Portal

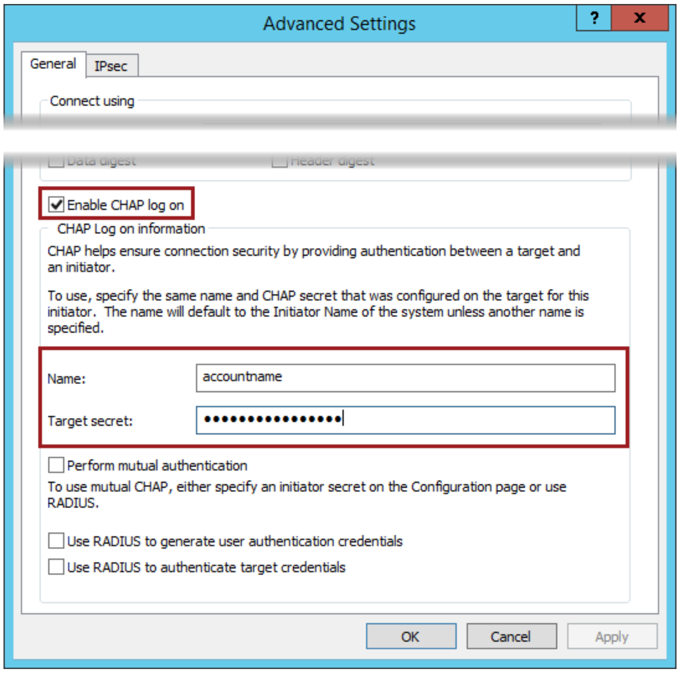
Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: <SolidFire SVIP>

Port: (Default is 3260.) 3260

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.



☑ Enable CHAP log on

CHAP Log on information

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.

Name: accountname

Target secret: ••••••••••••••••

□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

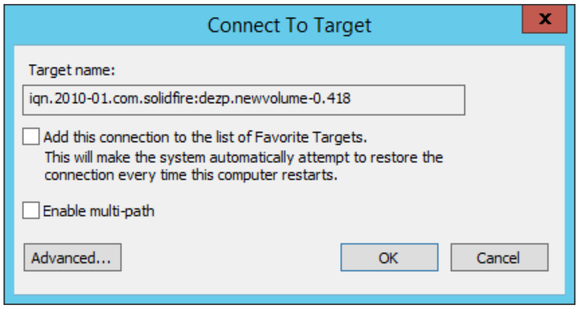
10. Click the Enable CHAP Log On check box to select it.
11. Enter the user name (SolidFire account name) and target secret (SolidFire initiator secret).

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

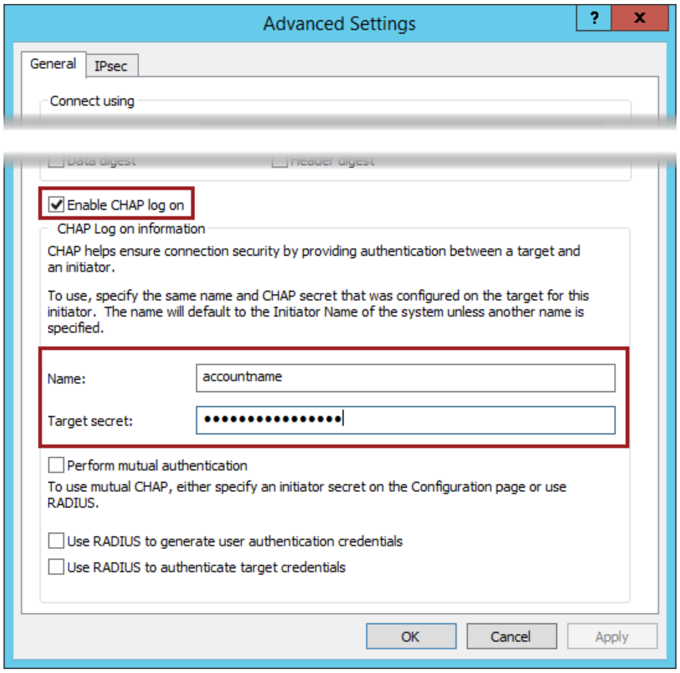


Target name: iqn.2010-01.com.solidfire:dezp.newvolume-0.418

□ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

□ Enable multi-path

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



□ Data digest □ Header digest

☑ Enable CHAP log on

CHAP Log on information

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.

Name: accountname

Target secret: ••••••••••••••••

□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

17. Click the Enable CHAP Log On check box to select it.
18. Enter the user name (SolidFire account name) and target secret (SolidFire initiator secret).

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

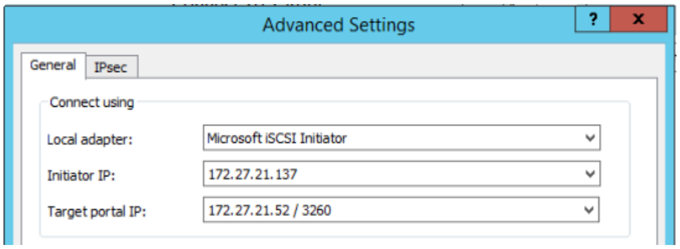
1. Install MPIO:
   a. Select Start > Control Panel > System and Security > Administrative Tools.
   b. Double-click Server Manager.
   c. In the Features area, click Add Features to open the Add Features Wizard.
   d. Click the Multipath I/O check box to select it.
   e. Click Next to open a confirmation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

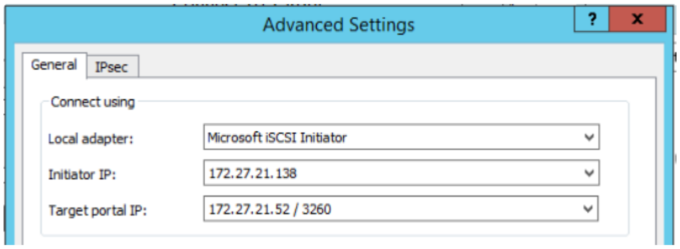


Local adapter: Microsoft iSCSI Initiator

Initiator IP: 172.27.21.137

Target portal IP: 172.27.21.52 / 3260

Figure 2) iSCSI login second path.



Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 172.27.21.138

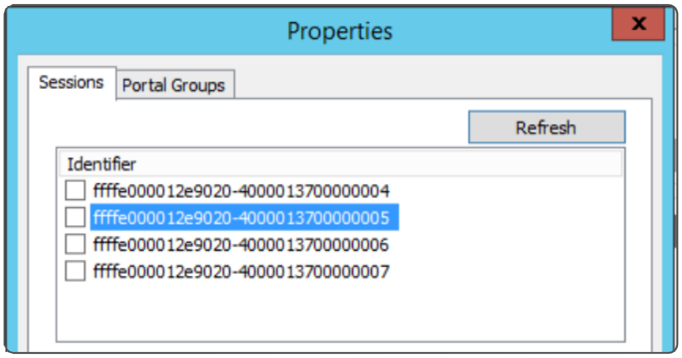
Target portal IP: 172.27.21.52 / 3260

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.



Identifier
- □ ffffe000012e9020-4000013700000004
- □ ffffe000012e9020-4000013700000005
- □ ffffe000012e9020-4000013700000006
- □ ffffe000012e9020-4000013700000007

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.

The system reboots automatically. When the reboot is complete, multipath is enabled.

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.

Note: See Creating Routing Tables.

2.5 Scanning for FC Volumes

After you have added the host WWPNs to the SolidFire volume access group, the volumes in that volume access group immediately become visible to the host. In order for the host to recognize the volumes, you must first scan the SCSI bus for the new volumes.

Prerequisites

- At least one volume has been added to the configured volume access group.
- All host WWPNs have been zoned to the SolidFire cluster and added to the configured volume access group.
- The MPIO Windows feature is installed.

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. If your FC volumes are not listed, right-click Disk Management and select Rescan Disks.

   Note: It is common to see multiple disks for a single connected SolidFire FC volume if MPIO has not been installed. If this happens, use the previous instructions to install MPIO and then rescan your disks.

2.6 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.

2.7 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 also 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	`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">http://technet.microsoft.com/enus/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
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.

2.8 Tuning Disk and iSCSI Timeouts

By default, Microsoft Windows disk timeouts are tuned for dir ectly 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 also 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	`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	`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)
Entry	`HKLM\System\CurrentControlSet\Services\mpio\Parameters\PathVerificationPeriod`
Default	30

iSCSI Values

Entry	`HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\<Instance ID>\Parameters\MaxRequestHoldTime`
Action	Set value to 90
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
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

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 SolidFire 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.

Min 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 SolidFire 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 Configuring SolidFire Quality of Service Guide or the Defining SolidFire Quality of Service Guide 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. You should verify the default queue depth before changing it, in case you want to revert back.

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, elxsor, 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.

Prerequisite

- hdparm version 9.x or higher can be used to set the queue depth.

  If you don't meet this requirement, you can use the node at `/sys/block/sdX/device/queue_depth` to read and set the queue depth values. The hdparm tool is not strictly required.

4 Creating the Partition and Formatting the Volume

You must configure iSCSI volumes connected to Microsoft Windows servers as online, initialized, and formatted in order 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 SolidFire iSCSI volumes.

4.2 Procedure

1. Initialize the disk:

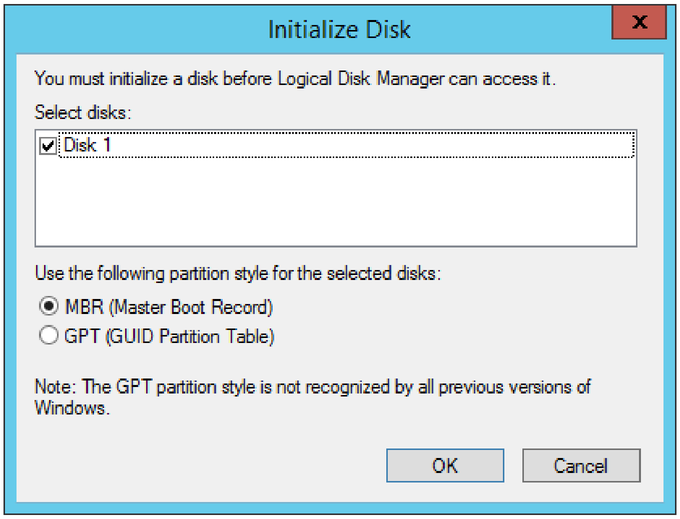
   a. Click Start > Control Panel > System and Security > Administrative Tools > Computer Management to open the Computer Management window.

   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.



You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1

Use the following partition style for the selected disks:

● MBR (Master Boot Record)

○ GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

   f. Select MBR or GPT.
   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 SolidFire documents or products in general, contact NetApp support 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://mysupport.netapp.com/info/web/ECMLP2740378.html

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

Trademark Information

TR-4643-1017