

iSCSI Initiator for Microsoft Windows Server 2008

OVERVIEW

This document is a compilation of many Best Practices guides that LeftHand Networks has compiled over years of implementing and selling iSCSI/IP Storage Networks. Although not an exhaustive set of Best Practices, the most common items seen in the field using the Microsoft iSCSI Initiator against a SAN/iQ enabled SAN are described in detail. This document pertains only to Windows 2008 running SAN/iQ software version 7.0 or higher. For information on best practices for Windows 2000 and Windows 2003, as well as previous versions of SAN/iQ, refer to the Application Note “[Best Practices for Enabling Microsoft® Windows with SAN/iQ](#)” available on the LeftHand Networks Resource Center.

CONTENTS

Enabling LeftHand SAN Volumes with the Microsoft iSCSI Initiator	3
Assign a Virtual IP Address to the LeftHand Cluster	3
Configuring the Microsoft iSCSI Initiator (Windows 2008 GUI).....	4
Configuring the Microsoft iSCSI Initiator (Windows 2008 Server Core).....	5
Adding Servers to the SAN/iQ Management Group for use with iSCSI.....	5
Assign Volumes and Snapshots to the Server	6
Enter Target Portal (VIP) Information	7
Mounting a Volume to a server.....	7
Mounting a Volume to Windows 2008 Server Core	8
Quick Commands	9
Challenge Authentication Protocol (Optional).....	10
Registering a Server and Target Portal with CHAP	10
Mounting a Volume to a Server with CHAP	11
Setting up the Initiator Secret.....	11
Setting up the Initiator Secret Through the Command Line.....	11
Mounting a Volume to a Server With CHAP through the GUI.....	11
Mounting a Volume to a server With CHAP through the Command Line.....	12
Creating Partitions and Formatting Volumes.....	13
SAN/iQ Thin Provisioning and Windows Volume Formatting Options	13
Creating a Partition with Disk Manager.....	13
Creating a Partition with Diskpart.....	17
Formatting a Volume from the Command Line	17
Dynamic Disks on A LeftHand SAN	18
Additional Documentation	18
Ensure That Application Resources on iSCSI Volumes Come Online After a Server Reboot	19
Setting up the Service Dependency with sc.exe	19
Verify Dependency Settings	19
Configuring Persistent Logons to the Target	20

Verify Persistence Settings	20
Microsoft iSCSI Initiator Session Timeout Setting.....	21
Setting the Session Timeout.....	22
Creating the MaxRequestHoldTime Value	23
Expanding a Windows Volume on the SAN.....	24
Increasing the Volume Size via the CMC.....	24
Increasing the Volume Size in Windows Via Disk Manager.....	24
Additional Documentation.....	26
Shrinking a Windows Volume on the SAN	27
Shrinking Volumes on the SAN.....	27
Shrinking Volumes on the SAN in Windows 2008 Server Core.....	30
Measuring Performance in a Windows Environment	31
Using Windows Performance Monitor to Measure SAN Performance.....	31
Setting up Windows Performance Monitor.....	32
Saving A Performance Monitor Log for Analysis.....	33
Monitoring more than one server simultaneously	35
Scheduling performance data collection	36
Configuring the iSCSI Volume.....	37
Configuring IOMeter	37
Configuring IOMeter Access Specification for each test.....	38
Running the Test.....	38
Interpreting Results.....	39
Access Specifications to Run.....	39
Frequently Asked Questions.....	40
Microsoft Windows 2008 Server	40
Microsoft MPIO.....	40
LeftHand Networks' Windows Solution Pack	40
Appendix A: Changes for Windows 2008	41
Appendix B: Commonly Used Commands for Setting up and Configuring a Windows 2008 Core Server	42
Appendix C: Finding the iSCSI Initiator Version	44

Enabling LeftHand SAN Volumes with the Microsoft iSCSI Initiator

OVERVIEW

The basic steps to connect a volume from the SAN to a server are below; detailed information follows in later sections:

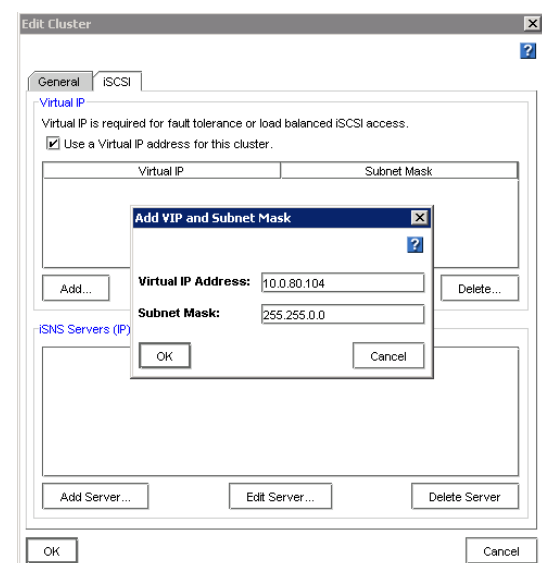
1. Assign the SAN/iQ cluster a Virtual IP Address (VIP), accomplished under the Edit Cluster task options.
2. Create the volume on the SAN
3. Create a Volume List which contains all the volumes that will mount to a particular server
4. Create an Authentication Group for the specified Windows server and associate it with the Volume List
5. Authentication Group should be for iSCSI volumes only
6. Authentication Group will need either the IQN of the server or CHAP information. If you are using CHAP see CHAP section below
7. In the iSCSI initiator, enter the Virtual IP Address into Target Portal address field under the Discovery tab to discover the volumes assigned in step 4.
8. Steps 4 and 5 must be completed for the iSCSI target discovery to work.
9. Logon/Connect to the volume as persistent (optional, persistence automatically restores the connection on reboot) in the iSCSI initiator under the Targets tab.
10. Format the volume
11. Set the service dependencies
12. Bind the volumes through the iSCSI initiator

DETAILED INSTRUCTIONS

Assign a Virtual IP Address to the LeftHand Cluster

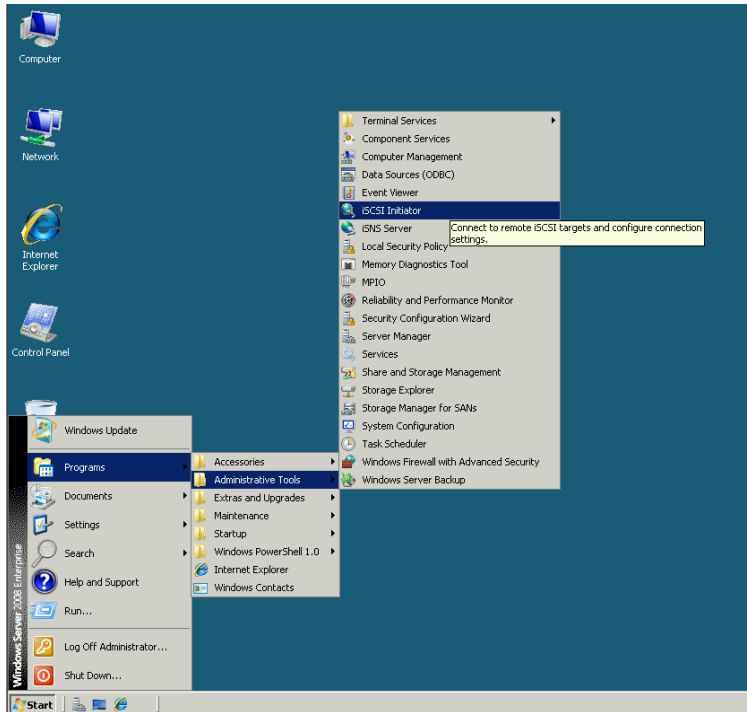
The VIP address provides a single client access point to the SAN for iSCSI session management. The VIP moves transparently between nodes in the event that the node holding the VIP becomes inaccessible. The VIP allows for increased availability and performance (through VIP load balancing). To assign a Virtual IP Address follow the steps below:

1. Open the Centralized Management Console and log into the Management Group in which the cluster resides
2. Right-click on the Cluster name, and select the Edit Cluster item
3. Select the iSCSI tab in the upper left
4. Enter the virtual IP address information of the cluster. The gateway information is not necessary if the servers are on the same subnet as the NSMs.
5. Click on OK

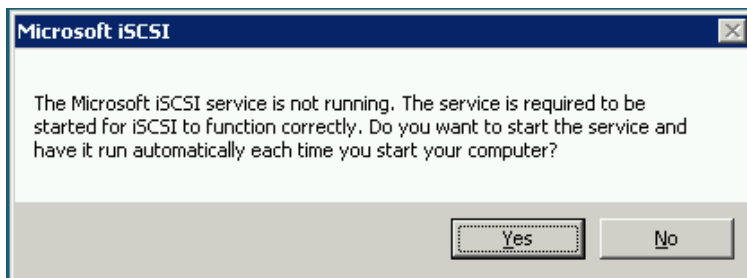


Configuring the Microsoft iSCSI Initiator (Windows 2008 GUI)

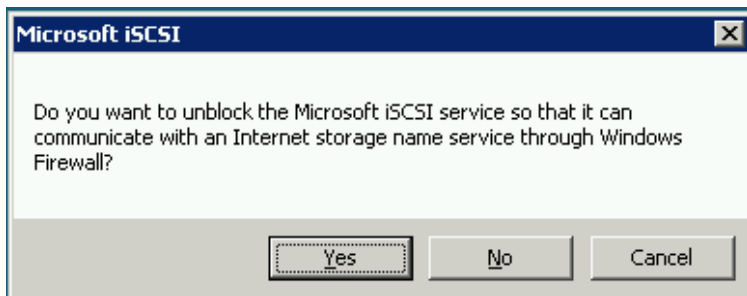
The Microsoft iSCSI initiator comes installed with Windows 2008. Previous versions of Windows would require the system administrator to download the initiator from Microsoft and install it manually. To upgrade to a newer releases of the initiator would require the system administrator to repeat the process. With Windows 2008, upgrades to the iSCSI initiator are done through the Windows Update process.



The first time you run the iSCSI initiator applet, the following dialog box will appear. Choose yes to start the iSCSI service and have it start automatically on boot.



A second dialog box appears. If you are using iSNS, select yes to allow iSNS traffic to pass through the Windows Firewall. Otherwise you can choose to keep those ports closed for better security.



Configuring the Microsoft iSCSI Initiator (Windows 2008 Server Core)

The first time a Windows 2008 Server Core system is connected to a LeftHand SAN, the Microsoft iSCSI service must be started. To do this, type the following at the command prompt:

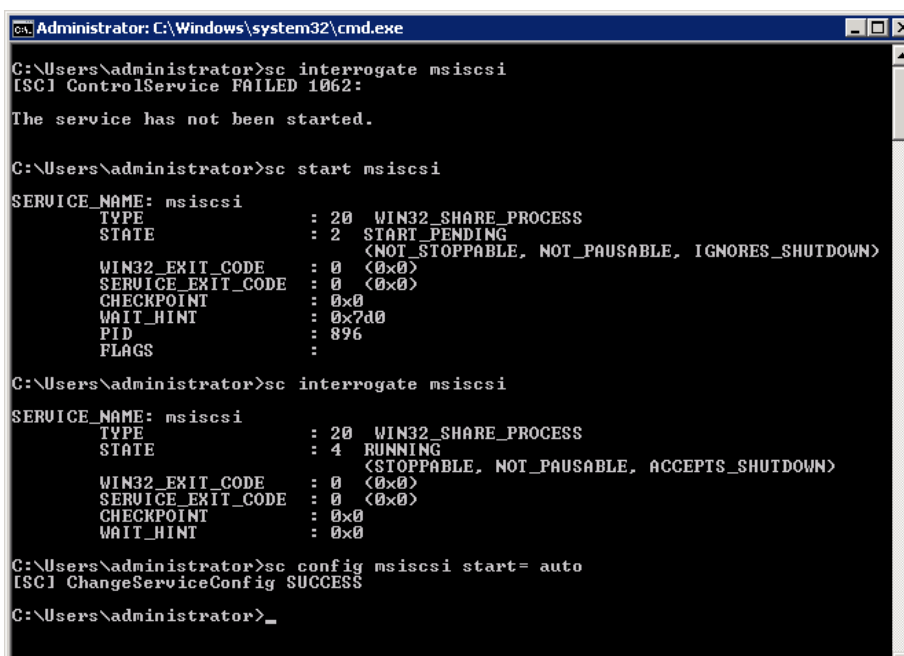
```
sc start msiscsi
```

At any time you can find the status of the service by using the interrogate command. To find the status of the iSCSI service, type the following from the command prompt:

```
interrogate msiscsi
```

To have the service start automatically on boot, type the following at the command prompt:

```
sc config msiscsi start= auto
```



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator>sc interrogate msiscsi
[SC] ControlService FAILED 1062:

The service has not been started.

C:\Users\administrator>sc start msiscsi

SERVICE_NAME: msiscsi
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 2   START_PENDING
                        (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 896
        FLAGS                 :

C:\Users\administrator>sc interrogate msiscsi

SERVICE_NAME: msiscsi
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 4   RUNNING
                        (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

C:\Users\administrator>sc config msiscsi start= auto
[SC] ChangeServiceConfig SUCCESS

C:\Users\administrator>
```

There is no need to configure the Windows Firewall from Windows 2008 Core to allow iSCSI traffic.

Adding Servers to the SAN/iQ Management Group for use with iSCSI

Add each server connection that needs access to a volume to the management group where the volume exists. Once you add a server connection to a management group, you can assign the server connection to one or more volumes or snapshots.

To register a Server, select the Tasks option from the Centralized Management Console (CMC) menu bar, go to Server, and select New Server. Enter the Server name, description and verify that the 'Allow access via iSCSI' and 'Enable load balancing' options are selected. Copy the initiator node name from the General tab on the iSCSI Initiator Properties from the Windows server into the matching field in the CMC and click Ok to complete the server registration.

New Server

Name:

Description:

iSCSI Security

☒ Allow access via iSCSI

☒ Enable load balancing [\(Information on compliant initiators\)](#)
Enabling load balancing on non-compliant initiators can compromise volume availability.
To function correctly load balancing requires that the cluster virtual IP be configured.

Authentication

☒ CHAP not required

Initiator Node Name:
[How do I find my initiator node name?](#)

☐ CHAP required

CHAP Name:

Target Secret:

Initiator Secret:

OK Cancel

iSCSI Initiator Properties

Favorite Targets | Volumes and Devices | RADIUS

General | Discovery | Targets

iSCSI devices are disk, tapes, CDs, and other storage devices on another computer on your network that you can connect to.
Your computer is called an initiator because it initiates the connection to the iSCSI device, which is called a target.

Initiator Name: [Change...](#)

To rename the initiator, click Change.

To use mutual CHAP authentication for verifying targets, set up a CHAP secret. [Secret](#)

To set up IPsec tunnel mode addresses, click Set up. [Set up](#)

[What is iSCSI ?](#)

OK Cancel Apply

Assign Volumes and Snapshots to the Server

Select the Tasks option from the CMC menu bar, go to Server, and select 'Assign and Unassign Volumes and Snapshots'. Select the volumes or snapshots to be accessed by the server, set the correct read/write permissions and click Ok.

Assign and Unassign Volumes and Snapshots

Choose volumes and snapshots to assign to server 'training12'.

Volume or Snapshot Name	Assigned	Permission
<input checked="" type="checkbox"/> Log_1	<input checked="" type="checkbox"/>	Read/Write
<input checked="" type="checkbox"/> Log_2	<input type="checkbox"/>	Read/Write
<input checked="" type="checkbox"/> Log_3	<input type="checkbox"/>	Read/Write
<input checked="" type="checkbox"/> SG_1	<input checked="" type="checkbox"/>	Read/Write
<input checked="" type="checkbox"/> SG_2	<input type="checkbox"/>	Read/Write
<input checked="" type="checkbox"/> SG_3	<input type="checkbox"/>	Read/Write

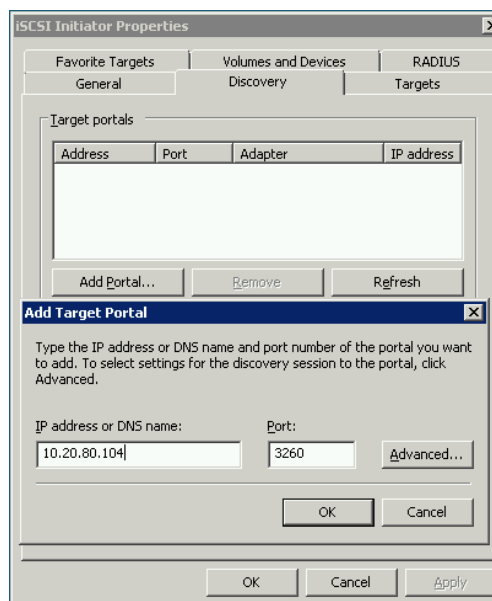


With the exception of Microsoft Failover Clusters, it is recommended to avoid allowing write access to a given volume by more than one host server to eliminate the possibility of data corruption. Thus, take caution to ensure that each volume is accessible by only one host server.

Enter Target Portal (VIP) Information

Once the volume list and authentication groups have been successfully created, add the Virtual IP address of the SAN/iQ cluster to the Target Portal list in the iSCSI initiator.

1. Double click on the iSCSI initiator icon
2. Select the Discovery tab
3. In the Target Portals section, click Add
4. Type in the IP Address of the Virtual IP of the cluster, leave the Port set to 3260, and click OK
5. Click OK
6. This establishes communication between the SAN and the server.

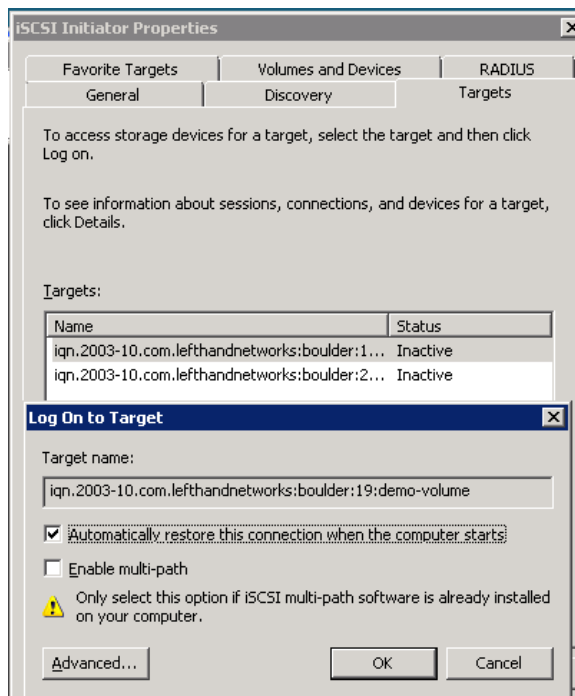


Mounting a Volume to a server

Select the Targets tab in the iSCSI initiator to view the targets. Locate the first volume you wish to connect to the server, it will be in an Inactive state, and select Log On. This will bring up the Log On to Target window. Click on the Automatically Reconnect at reboot box and select OK. This checkbox will insure that the volume automatically connects upon server reboot. The volume should now show as Connected.

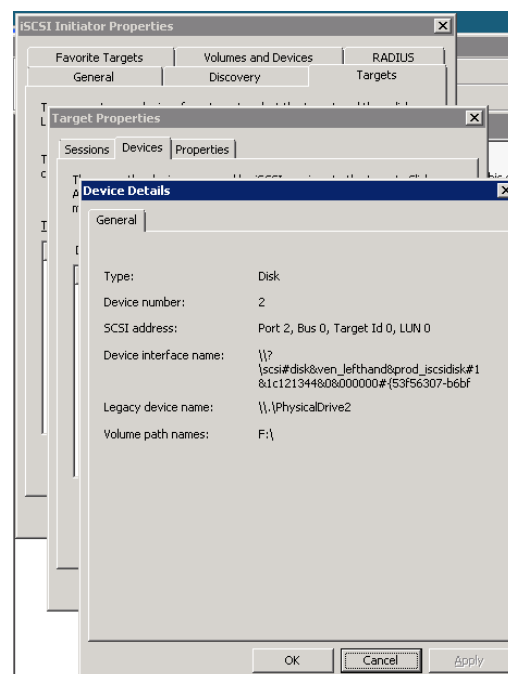
You will only see the volumes which have been assigned to the server in the CMC.

If you do not see your volumes listed, first click on the Refresh button, then check the volume and Virtual IP address configurations.



Do not select the "Enable Multi-path" checkbox unless you are using a supported version of the LeftHand Networks DSM for MPIO to enable multiple iSCSI initiators in the server.

To view the details about the newly established volume, and trace the volume from the SAN to the server, select the volume then click the Details button – this will bring up the Target Properties window. Next, click the Devices tab then the Advanced button. This will bring up the Device Details screen shown below, which shows the disk number assigned to the volume by the server, as seen under Disk Management. Use this as needed to trace volumes from the SAN to the server.



Mounting a Volume to Windows 2008 Server Core

In Windows 2008 Server Core, the volume must be mounted via the command line, using a built-in tool called `iscsicli.exe`. First, add the target portal. The syntax for adding a portal is:

```
AddTargetPortal <TargetPortalAddress> <TargetPortalSocket><Initiator Instance
Name> <Initiator Port Number><Security Flags><Login Flags> <Header Digest>
<Data Digest> <Maximum Connections> <DefaultTime2Wait> <DefaultTime2Retain>
<Username> <Password> <AuthType>
```

Typically, the only values that need to be passed are the portal IP address and the portal socket. The other values can be used for specific use cases which are outside the scope of this document. As an example, a typical command to add the target portal might look like the following:

```
AddTargetPortal 10.0.80.104 3260
```

The syntax for mounting a volume is as follows:

```
LoginTarget <TargetName> <ReportToPNP><TargetPortalAddress><TargetPortalSocket>
<Initiator Instance Name> <Port number> <Security Flags> <Login Flags> <Header
Digest> <Data Digest> <Max Connections> <DefaultTime2Wait> <DefaultTime2Retain>
<Username> <Password> <AuthType> <Key> <Mapping Count> <Target Lun> <OS Bus>
<Os Target> <OS Lun>
```

For each parameter being passed, and asterisk (*) can be used to indicate that the default value should be used. As an example, a typical command to log in to a volume might look like the following:

```
logintarget iqn.2003-10.com.lefthandnetworks:boulder:23:demo-volume2 T * *
Root\ISCSIPRT\0000_0 10.0.80.104 3260 * * * * * * * * * 0
```



```
Administrator: C:\Windows\system32\cmd.exe - iscsi
C:\>iscsi
Microsoft iSCSI Initiator Version 6.0 Build 6000

[iqn.1991-05.com.microsoft:windows2008core] Enter command or ^C to exit
logintarget iqn.2003-10.com.lefthandnetworks:boulder:23:demo-volume2 T * * Root
\ISCSIPRT\0000 0 10.0.80.104 3260 * * * * * 0
Session Id is 0xfffffa80047da018-0x4000013700000004
Connection Id is 0xfffffa80047da018-0x4
The operation completed successfully.
[iqn.1991-05.com.microsoft:windows2008core] Enter command or ^C to exit
```

To log out of a volume, use the LogoutTarget command. Syntax of the command is:

LogoutTarget <SessionID>

For this example, the command to log out of the volume would be:

LogoutTarget 0xfffffa80047da018-0x4000013700000004

To find out which sessions are currently active, use the following command:

SessionList

```
Administrator: C:\Windows\system32\cmd.exe - iscsi
C:\>iscsi
Microsoft iSCSI Initiator Version 6.0 Build 6000

[iqn.1991-05.com.microsoft:windows2008core] Enter command or ^C to exit
logouttarget 0xfffffa80047da018-0x4000013700000004
The operation completed successfully.
[iqn.1991-05.com.microsoft:windows2008core] Enter command or ^C to exit
```

NOTES:

- To have the volumes mount automatically at boot, they must be a persistent (favorite) login. The syntax for logging in to a target and persistently logging in to a target is the same, just the command is different. Instead of “LoginTarget” use “PersistentLoginTarget” and instead of “LogoutTarget” use “RemovePersistentTarget. To verify persistent targets, use the command “ListPersistentTargets” – all targets marked as persistent (favorites) will be displayed.

Next, go to the Windows Disk Management utility to create a volume and format the volume for use as a locally attached disk. Dynamic disks are supported with iSCSI in Windows 2008. This is a change from previous releases of Microsoft Windows. See

Quick Commands

The iscsi application also has several “quick commands” built in. These operate in much the same way as the standard commands, but are not passed as many variables. Instead, defaults are assumed except for those options that are typically unique in configuring access to storage. For example, the Target Portal Socket rarely changes from the default of 3260, but the Target Portal Address is typically unique between environments, sometimes with more than one instance per server. In this example, for the command “LoginTarget”, by using the Quick Command the syntax would change from:

```
logintarget   iqn.2003-10.com.lefthandnetworks:boulder:23:demo-volume2   T   *   *  
Root\ISCSIPRT\0000_0 10.0.80.104 3260 * * * * * * * * * * 0
```

to:

```
qlogintarget iqn.2003-10.com.lefthandnetworks:boulder:23:demo-volume2
```

More Quick Commands can be found by typing “iscsicli /help” from the command prompt, or “help” from the iscsicli shell.

Challenge Authentication Protocol (Optional)

Instead of using IQN security only (described above), one can also use the Challenge Authentication Protocol (CHAP). CHAP is a protocol that is used to authenticate the peer of a connection and is based upon the peer sharing a password and secret. The Microsoft iSCSI initiator service and LeftHand Networks SAN support both one-way and two-way mutual CHAP.

CHAP authentication uses secrets associated with both the target and the initiator. Any initiator wanting to access a volume must know the target secret and any target to be authenticated must know the initiator secret.

Setting up CHAP is a two part process. The first part is establishing an Authentication Group, the second step is connecting the volume. The following section details how to configure the Microsoft iSCSI initiator and LeftHand volume for CHAP Authentication.

Registering a Server and Target Portal with CHAP

To register a Server, select the Tasks option from the Centralized Management Console (CMC) menu bar, go to Server, and select New Server. Enter the Server name, description and verify that the ‘Allow access via iSCSI’ and ‘Enable load balancing’ options are selected. Copy the initiator node name from the General tab on the iSCSI Initiator Properties from the Windows server into the matching field in the CMC and click Ok to complete the server registration. Click the “CHAP required” radio button. Use the following steps to find and set the CHAP Name and Target Secret (see diagram below).

1. Open the iSCSI initiator and go to the Target Portals tab
2. Click on the Add button
3. Type in the Virtual IP Address of the cluster where the volume resides
4. Click on the Advanced button in the Add Target Portal window
5. In the Advanced Settings window, under the General tab, in the middle of the window click on the CHAP logon information check box
6. Cut and paste the User Name from the initiator into the CHAP Name box of the Server from the CMC. This name can be changed, by default it is the same as the IQN name.
7. In the New Server window, fill in the Target Secret and click OK.
8. In the iSCSI initiator, fill in the Target Secret (same as in step 7 above) and click OK.
9. Click OK in the Add Target Portal window. The server is now communicating with the SAN.

Mounting a Volume to a Server with CHAP

Select the Targets tab in the iSCSI initiator to view the targets.

Locate the first volume you wish to connect to the server machine, it will be in an Inactive state, and select Log On. This will bring up the Log On to Target window. Select the “Automatically restore this connection when the system boot” check box. This checkbox will insure that the volume automatically connects upon host server reboot.

Next, click on the Advance button. This will bring up the Advanced Settings window. Under the General tab, click the “CHAP logon information” check box, and fill in the CHAP name and Target secret information, and click OK. Click OK in the Log On to Target window, and in the iSCSI Initiators Properties windows. The volume should now show as Connected.

To view the details about the newly established volume, and trace the volume from the SAN to the server, select the volume then click the Details button – this will bring up the Target Properties window. Next, click the Devices tab then the Advanced button. This will bring up the Device Details screen, which shows the disk number assigned to the volume by the host system, as seen under Disk Management. Use this as needed to trace volumes from the SAN to the server. Next, go to the Disk Management utility and format the volume for use as a locally attached Basic Disk. Finally, set the service dependency and bind the volumes through the iSCSI initiator.

Setting up the Initiator Secret

The Initiator Secret is set at the MS iSCSI initiator and must be configured via the LeftHand CMC and the MS initiator interface. From the MS Initiator interface, create the initiator secret. The secret must be between 12 and 16 characters long and must be different than the target secret.

To configure the initiator secret open the iSCSI initiator interface and choose the Initiator Settings tab.

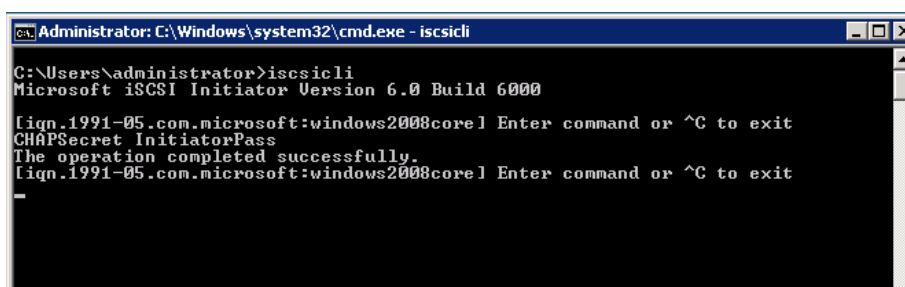
Assign a secret to the initiator. Record the initiator secret and the initiator node name. These will be used to complete the configuration via the CMC. The initiator node name may be cut and pasted.

The Initiator Secret is associated with the Server, open the Server you want to add the initiator secret to. Fill in the Initiator Secret and click OK.

Setting up the Initiator Secret Through the Command Line

From a command line or in Windows 2008 Core, the Initiator Secret can be set by using the following command:

```
CHAPSecret <CHAP secret>
```



```
Administrator: C:\Windows\system32\cmd.exe - iscsicli
C:\Users\administrator>iscsictl
Microsoft iSCSI Initiator Version 6.0 Build 6000
[logn.1991-05.com.microsoft:windows2008core] Enter command or ^C to exit
CHAPSecret InitiatorPass
The operation completed successfully.
[logn.1991-05.com.microsoft:windows2008core] Enter command or ^C to exit
```

Mounting a Volume to a Server With CHAP through the GUI

Select the Targets tab in the iSCSI initiator to view the targets.

Locate the first volume you wish to connect to the server, it will be in an Inactive state, and select Log On. This will bring up the Log On to Target window. Select the “Automatically restore this connection when the system boot” check box. This checkbox will insure that the volume automatically connects upon server reboot.

Next, click on the Advanced button. This will bring up the Advanced Settings window. Under the General tab, click the “CHAP logon information” check box, and fill in the CHAP name and Target secret information, and click OK. Click OK in the Log On to Target window, and in the iSCSI Initiators Properties windows. The volume should now show as Connected.

To view the details about the newly established volume, and trace the volume from the SAN to the server, select the volume then click the Details button – this will bring up the Target Properties window. Next, click the Devices tab then the Advanced button. This will bring up the Device Details screen shown on page nine, which shows the disk number assigned to the volume by the server, as seen under Disk Management. Use this as needed to trace volumes from the SAN to the server.

Next, go to the Disk Management utility and format the volume for use as a locally attached disk.

Finally, set the service dependency and bind the volumes through the iSCSI initiator.



This is a critical step to prevent applications from trying to start prior to their volumes being present. Performing this step will delay the start of applications until their bound volumes are present.

Mounting a Volume to a server With CHAP through the Command Line

Mounting a volume with CHAP through the command line is similar to mounting a volume through the command line without CHAP. First, set the initiator secret using the command ChapSecret. For example:

```
ChapSecret <InitiatorSecret>
```

Using QLoginTarget (LoginTarget would work as well), simply pass the target name, CHAP Name, and CHAP password when executing the command. For example:

```
QloginTarget iqn-2003-10.com.lefthandnetworks:boulder:23:demo-volume-2 CHAPName  
TargetPassword
```

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator>iscsi
Microsoft iSCSI Initiator Version 6.0 Build 6000
iqn.1991-05.com.microsoft:windows2008core1 Enter command or ^C to exit
QAddTargetPortal 10.0.80.104 CHAPName TargetPassword
The operation completed successfully.
iqn.1991-05.com.microsoft:windows2008core1 Enter command or ^C to exit
QLoginTarget iqn.2003-10.com.lefthandnetworks:boulder:23:demo-volume-2 CHAPName T
argetPassword
Session Id is 0xfffffa80047d8438-0x4000013700000004
Connection Id is 0xfffffa80047d8438-0x3
The operation completed successfully.
iqn.1991-05.com.microsoft:windows2008core1 Enter command or ^C to exit
C:\Users\administrator>_
```

Creating Partitions and Formatting Volumes

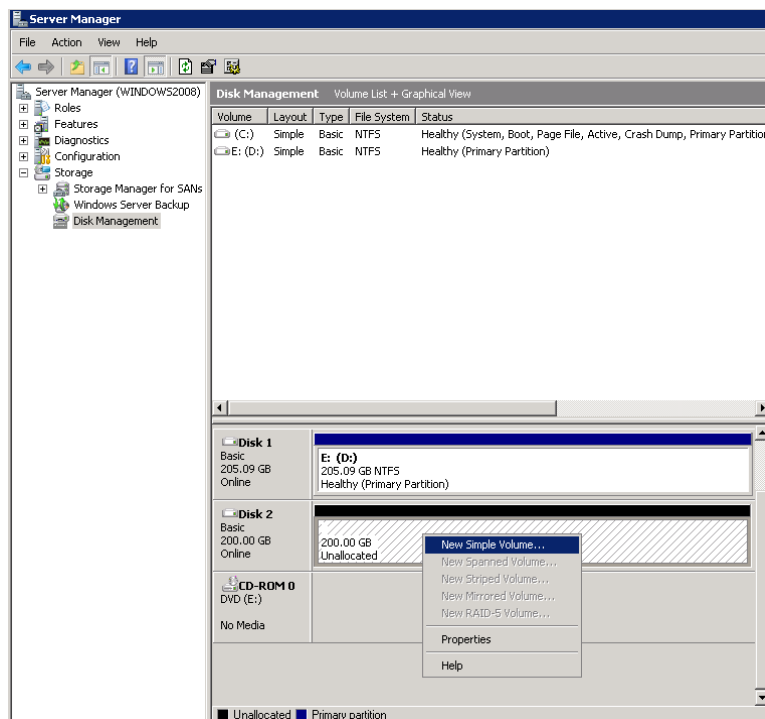
SAN/iQ Thin Provisioning and Windows Volume Formatting Options

SAN/iQ Thin Provisioning allows volumes to be created in the SAN without pre-allocating storage space. This feature greatly increases the overall utilization of the SAN and removes the challenge of predicting future storage requirements. Storage space is allocated as data is written to the volume. Easy-to-read charts and alerts keep you apprised of volume utilization levels, letting you know when you are approaching storage limits and allowing you to purchase storage capacity when you need it.

Windows Server 2008 writes to the entire disk when performing a full format whereas previous versions of Windows performed a read. Microsoft and LeftHand Networks both recommend performing a quick format when using on-demand allocating modes such as SAN/iQ Thin Provisioning. This avoids the initial write to the entire disk, maintains on-demand utilization and completes in seconds rather than minutes to hours for large disks.

Creating a Partition with Disk Manager

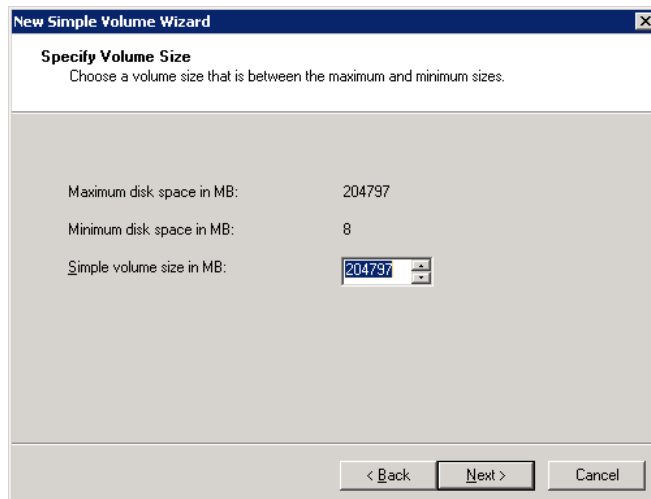
To create a partition and format a drive, start Disk Manager by going into Server Manager, expanding the “Storage” header, and selecting “Disk Management”. The volumes that have been created and mounted by the server will appear on the bottom right of Disk Manager. They will be online and unallocated. Creating a partition and formatting the volume are done in one process. To begin this process, right click the un-partitioned volume and select “New Simple Volume.”



A wizard appears. Click on “Next”.



Another dialog box appears asking for the size of the volume to be created. By default, the maximum capacity of the volume will be filled in. In most cases the volume on the SAN was created to the proper size, so using the full capacity here would make the most sense.



NOTE:

- LeftHand Best Practices are to create a volume on the SAN that is the same size as the partition created in Windows. While it is acceptable and supported to create multiple partitions on the volume presented by the SAN, creating the volume as the same size as the partition allows more granularity for creating snapshots, remote copies, etc. It also eases management as a change to one volume and partition will not affect the other partitions on the volume.

Another dialog box appears, asking whether to assign a drive letter (and which letter), to mount the volume in an empty NTFS folder, or to not assign a drive letter or path. Consult with the application vendor to determine the proper option here.

New Simple Volume Wizard [X]

Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.

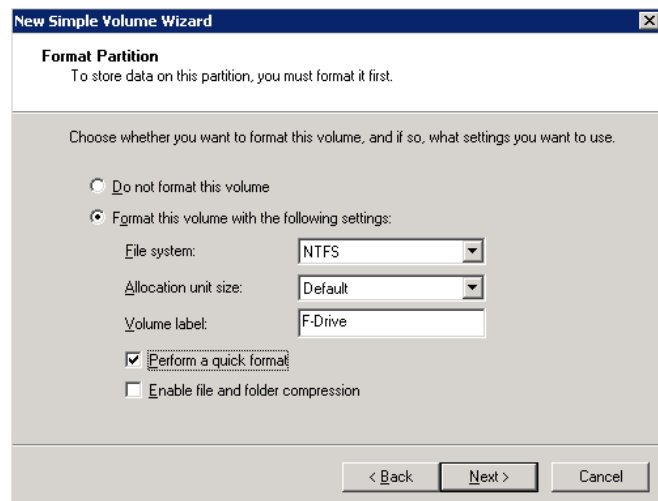
☒ Assign the following drive letter: F

☐ Mount in the following empty NTFS folder:
 Browse...

☐ Do not assign a drive letter or drive path

< Back Next > Cancel

A dialog box appears asking for information on formatting the volume. In some instances, the volume would not need to be formatted, but typically most applications require a formatted volume in order to access the disk. Unless otherwise directed by the application vendor, keep the default file system and allocation unit values. The volume label can be changed to something appropriate for the volume. For example, a volume that contains an Exchange database might be labeled “Exchange-DB”. The label exists to help identify volumes.



New Simple Volume Wizard

Format Partition
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS

Allocation unit size: Default

Volume label: F-Drive

☒ Perform a quick format

☐ Enable file and folder compression

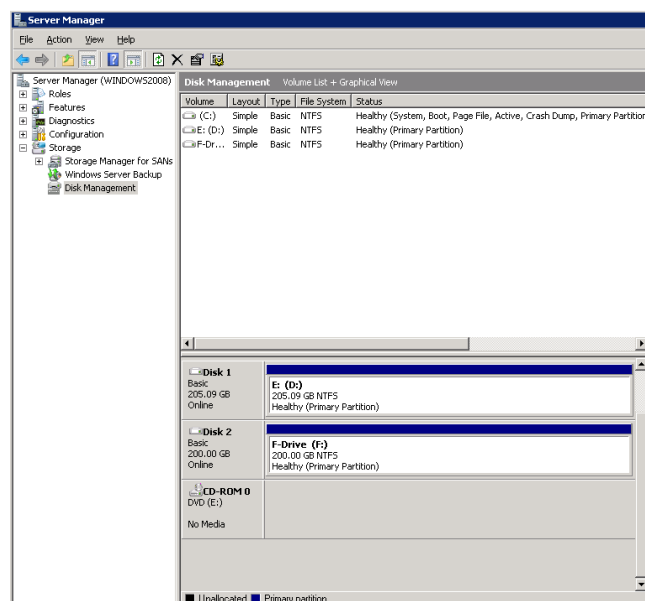
< Back Next > Cancel



It is a best practice to choose “Perform a Quick Format”. This allows the format to complete in seconds as opposed to several minutes or even hours for larger volumes. There is no benefit to doing a full volume format with a LeftHand SAN.

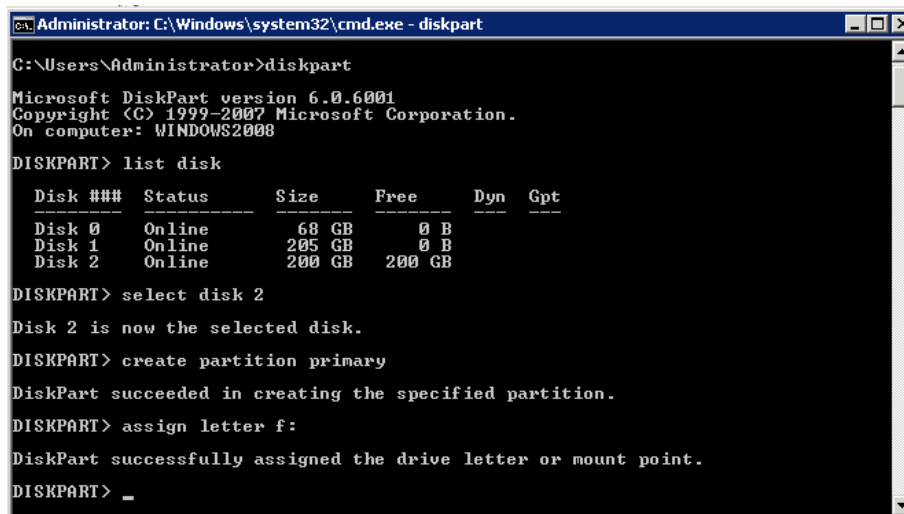
The final dialog box appears, showing the list of selections made so far. Click “Finish” to create the volume and perform the format, “Back” to go back and change an option, or “Cancel” to cancel the creation of the partition and formatting of the volume.

The volume now shows up as fully partitioned, with the appropriate drive letter and label.



Creating a Partition with Diskpart

1. Diskpart.exe is already available on a Windows 2008 server
2. Open a command prompt and type diskpart.exe
3. Enter > list disk
4. Note the disk number that you want to create the partition on.
5. Enter > select disk (disk number)
6. Enter > create partition primary
7. Enter > assign letter (the letter you want the drive to have)
8. Or enter > assign mount (the path of a empty dir to mount the drive to)
9. Enter > exit (to exit diskpart)



```
C:\Users\Administrator>diskpart
Microsoft DiskPart version 6.0.6001
Copyright (C) 1999-2007 Microsoft Corporation.
On computer: WINDOWS2008

DISKPART> list disk

   Disk ###  Status         Size           Free           Dyn  Gpt
   -----  -
   Disk 0      Online            68 GB             0 B
   Disk 1      Online           205 GB             0 B
   Disk 2      Online           200 GB           200 GB

DISKPART> select disk 2
Disk 2 is now the selected disk.

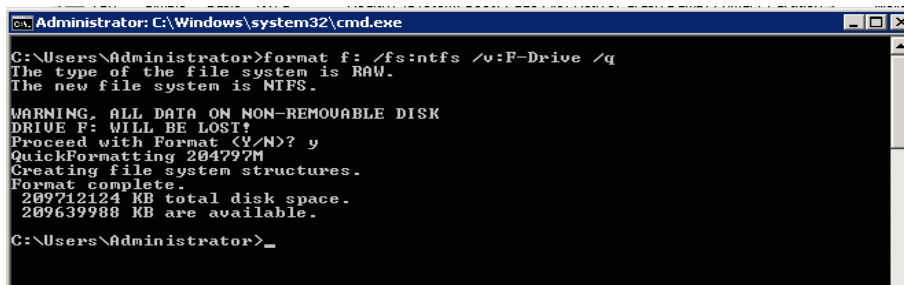
DISKPART> create partition primary
DiskPart succeeded in creating the specified partition.

DISKPART> assign letter f:
DiskPart successfully assigned the drive letter or mount point.

DISKPART> _
```

Formatting a Volume from the Command Line

1. Open a command prompt
2. Type the following command:
3. **format <drive letter> /fs:<file system> /v:<volume label> /q**, where f: is the volume to format, /fs: is the file system to be used, /v: is the volume label, and /q does a quick format.
4. Type “y” when asked whether to proceed with the format.



```
C:\Users\Administrator>format f: /fs:ntfs /v:F-Drive /q
The type of the file system is RAW.
The new file system is NTFS.

WARNING: ALL DATA ON NON-REMOVABLE DISK
DRIVE F: WILL BE LOST!
Proceed with Format (Y/N)? y
QuickFormatting 204797M
Creating file system structures.
Format complete.
209712124 MB total disk space.
209639988 MB are available.

C:\Users\Administrator>_
```

Dynamic Disks on A LeftHand SAN

With Windows 2008, dynamic disks are now supported over iSCSI. This is a change from previous versions of Windows. However, most of the functionality that dynamic disks support is found in the base SAN/iQ software. Also, there is additional resource utilization on the Windows server which comes from the management and operation of these dynamic disk sets. The following table refers to common use cases of dynamic disks.



LeftHand Networks does not support Snapshots or Remote Copies of the dynamic disks listed in the table below. For administrators that wish to use the Snapshot or Remote Copy functionality of the SAN it is highly recommended that they use the SAN/iQ functionality rather than Dynamic Disks.

Type of Dynamic Disk	Use Case	SAN/iQ Alternative
Spanned Volumes	Combine multiple physical spindles to create a volume that is larger than a single volume	SAN/iQ Virtualizes all physical spindles into a pool of resources, to that any one volume can access the storage capacity of all the drives. Additionally, thin provisioning allows administrators to present volumes to the Windows Server without reserving space on the SAN, maximizing SAN utilization.
Striped Volumes	Increase performance of storage by aggregating performance of all physical spindles	SAN/iQ Virtualizes all physical spindles into a pool of resources, to that any one volume can take advantage of the aggregate performance of all the drives.
Mirrored Volumes	Increase performance and availability of disk by creating a mirrored copy of the volume. This offers better performance but less capacity than RAID-5.	Hardware RAID 10 on the NSMs provides a highly redundant, high performance disk configuration. There is no need to add another layer of RAID on top of this.
RAID-5 Volumes	Increase capacity and performance of volumes by combining physical spindles and having a drive fail. This offers better capacity but less performance than Mirrored Volumes.	Hardware RAID 5 on the NSMs provides a highly available, high performance disk configuration. There is no need to add another layer of RAID on top of this.

Managing dynamic disks that are used in any of the above ways creates additional administrator overhead. Using software RAID from within Windows 2008 uses more system resources than simple Basic disks. Additionally, if a mirrored or striped volume is created, the user will not be able to extend or shrink the volume. For these reasons, LeftHand Networks recommends using Basic Disks within Windows Server 2008, and doing disk management and maintenance on the LeftHand SAN rather than from within Windows.

Additional Documentation

How to Align Exchange I/O with Storage Track Boundaries

http://www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3Perf_ScalGuide/0e24eb22-fbd5-4536-9cb4-2bd8e98806e7.mspx

A Description of the Diskpart Command-Line Utility <http://support.microsoft.com/default.aspx?scid=kb;en-us:300415>

Ensure That Application Resources on iSCSI Volumes Come Online After a Server Reboot

OVERVIEW

This section describes how to configure Windows servers with iSCSI so that volumes come online before applications that rely on them. Windows starts its services in order based upon dependencies. For applications like File Shares, Exchange, SQL, and Microsoft Clusters to come online smoothly at boot up their services need to be made dependent upon the Microsoft iSCSI Service. Once the service dependencies are correct iSCSI volumes also need to be bound by the iSCSI initiator. Binding volumes ensures that the iSCSI service waits for those volumes to come online before signaling that it is finished starting its service, then the dependant services can startup and the volumes they need will be available. The configuration involves three main steps and needs to be set up on all Windows servers that mount iSCSI volumes.

SETTING THE SERVICE DEPENDENCY

Windows starts its services in order based upon dependencies. For applications like Exchange, SQL, file shares, etc. to come online gracefully at boot up, their services need to be made dependent upon iSCSI. Some examples of Service Dependencies that may need to be dependent on iSCSI are:

Service	Service Name	Symptoms of iSCSI dependency issues
File shares	lanmanserver	Loss of access to file share volumes
Exchange	msexchangeis	Mail stores may become un-mounted
SQL Server	mssqlserver	Databases started as "suspect"



Take precautions to observe and preserve existing dependencies when setting iSCSI dependencies.

Setting up the Service Dependency with sc.exe

LeftHand recommends setting sc.exe to create dependencies rather than editing the registry. sc.exe is included with Server 2008 and can be run from an alternate network computer.

From a DOS prompt, type `sc config <your_service_name> depend= MSiSCSI`. For example: `sc config lanmanserver depend= MSiSCSI`. Alternately, perform this command from a networked computer if you have administrative access to the server. To do this, type `sc \\computer_name config LanManServer depend= MSiSCSI`.

You must use the real name of a service, not the display name. For example, use "lanmanserver" as opposed to simply "Server" or "file shares". A list of all applicable service names is available by typing "sc query | more" from a DOS prompt.

Verify Dependency Settings

1. Right-click on My Computer and select Manage.
2. In the Computer Management window, expand Services_and_Applications and select Services.
3. Double-click the applicable service. The applicable service could be "Server" for file shares, "MSSQLSERVER" for SQL, "Microsoft Exchange Information Store" for Exchange, etc.
4. Select the Dependencies tab for the service and confirm that Microsoft iSCSI Initiator is listed in the box labeled.

CONFIGURING PERSISTENT LOGONS TO THE TARGET

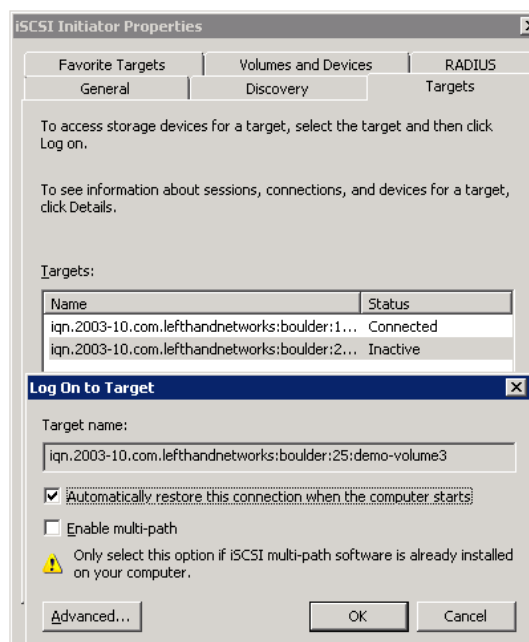
Making the target persistent ensures that the iSCSI service automatically logs in to the target and activates the connection at boot up.

Configuring Persistent Logons to the Target

1. Open Control Panel and double-click the iSCSI Initiator.
2. Select the Available Targets or Targets tab, depending on the version of the iSCSI initiator you are using.
3. Select a target in the list, and then click Log On.
4. Select the Automatically restore this connection when the system boots check box, then click OK.

Verify Persistence Settings

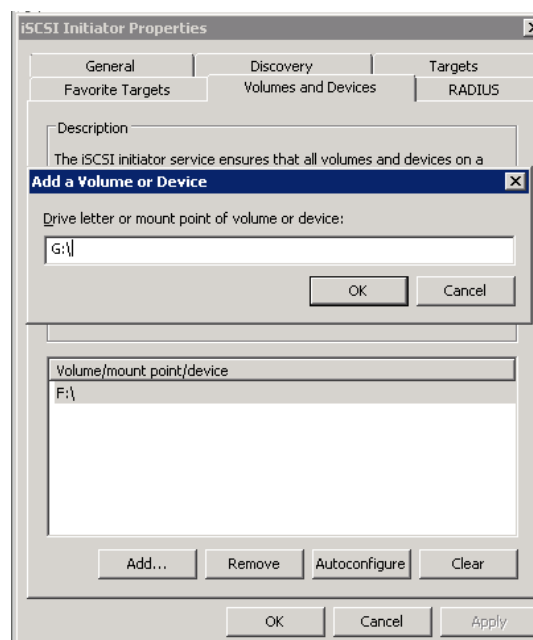
1. Open Control Panel and double-click the iSCSI Initiator.
2. Select the Persistent Targets tab and confirm that the volume name / Target IQN is included in the list.



BINDING VOLUMES WITH THE MICROSOFT ISCSI INITIATOR

Once iSCSI Dependencies and Persistent Logons are configured, and connectivity with the server is confirmed, the final step is to bind the volumes in the iSCSI initiator.

1. Open Control Panel and double-click the iSCSI Initiator.
2. Select the Volumes and Devices tab.
3. Click Autoconfigure.
4. Confirm that the Volume/Mount Point/Device window has a drive letter entry for each volume.
5. Click OK to close the iSCSI Initiator.



NOTES:

- Binding the volumes always needs to be the final step in this process. If you do these steps out order, or if you add subsequent servers or volumes, bind the volumes again as a final step, otherwise the volumes may not be available after the server reboot.
- If the entry in the Bound Volumes/Devices tab is anything other than a simple drive letter, remove the entries, mount the volumes, check all network settings, etc., and try binding again. Properly mounted volumes should always show up as a simple drive letter in the Bound Volumes/Devices tab.

Microsoft iSCSI Initiator Session Timeout Setting

OVERVIEW

The Microsoft iSCSI Initiator session failover timeout is set to 60 seconds by default. This default timeout period is generally too short to accommodate all iSCSI failover delays that may occur. For example, iSCSI failover events and associated delays can be triggered by storage module reboots/upgrades, network outages, power outages, etc. If the iSCSI session failover time exceeds the timeout period, the Initiator can go into a reconnect state, resulting in potential loss of connectivity for any pending I/O operations, resulting in those I/Os being flushed from the server cache.

To prevent this reconnect state from happening, the Initiator timeout value should be increased on every system that has an iSCSI volume. LeftHand Networks recommends that this timeout value be set to 10 minutes (600 seconds). The timeout for the Microsoft iSCSI Initiator is controlled via a Microsoft iSCSI Registry entry named `MaxRequestHoldTime`.

NOTES:

- With SAN/iQ 6.6.x or earlier, or with any version of SAN/iQ when the LeftHand DSM for MPIO is not being used, if the Microsoft DSM is installed during the iSCSI initiator setup, a separate 30 second iSCSI failover timeout is used instead of the `MaxRequestHoldTime` value, which is ignored. This 30 second timeout value can have adverse affects on iSCSI volume and data availability (see below). Therefore it is critical to uninstall the Microsoft DSM in these situations.
- Starting with SAN/iQ version 7.0, the iSCSI timeouts on the SAN have been reduced such that changing the `MaxRequestHoldTime` is technically no longer necessary. However, in order to compensate for iSCSI issues outside of SAN control, such as network disturbances, etc., LeftHand still recommends changing the `MaxRequestHoldTime` value to 600 seconds.
- Any time the iSCSI initiator is reinstalled or upgraded, the `MaxRequestHoldTime` value may revert to its default value of 60 seconds. Always reconfirm this setting after reinstalling or upgrading the initiator.
- The `MaxRequestHoldTime` value should be modified on every Windows system with an iSCSI volume. This recommendation also applies to cluster nodes using iSCSI resources in Microsoft Cluster Service (MSCS).



LeftHand Networks does not recommend setting `MaxRequestHoldTime` to FFFFFFFF (i.e., infinite). The downside of using the infinite setting for `MaxRequestHoldTime` is that the server's cache memory may become full with pending iSCSI data that is waiting to be written to the SAN, which can result in a degradation of server performance – and can lead to a complete lock up of the system. For that reason, LeftHand Networks recommends setting `MaxRequestHoldTime` to 600 seconds (10 minutes).

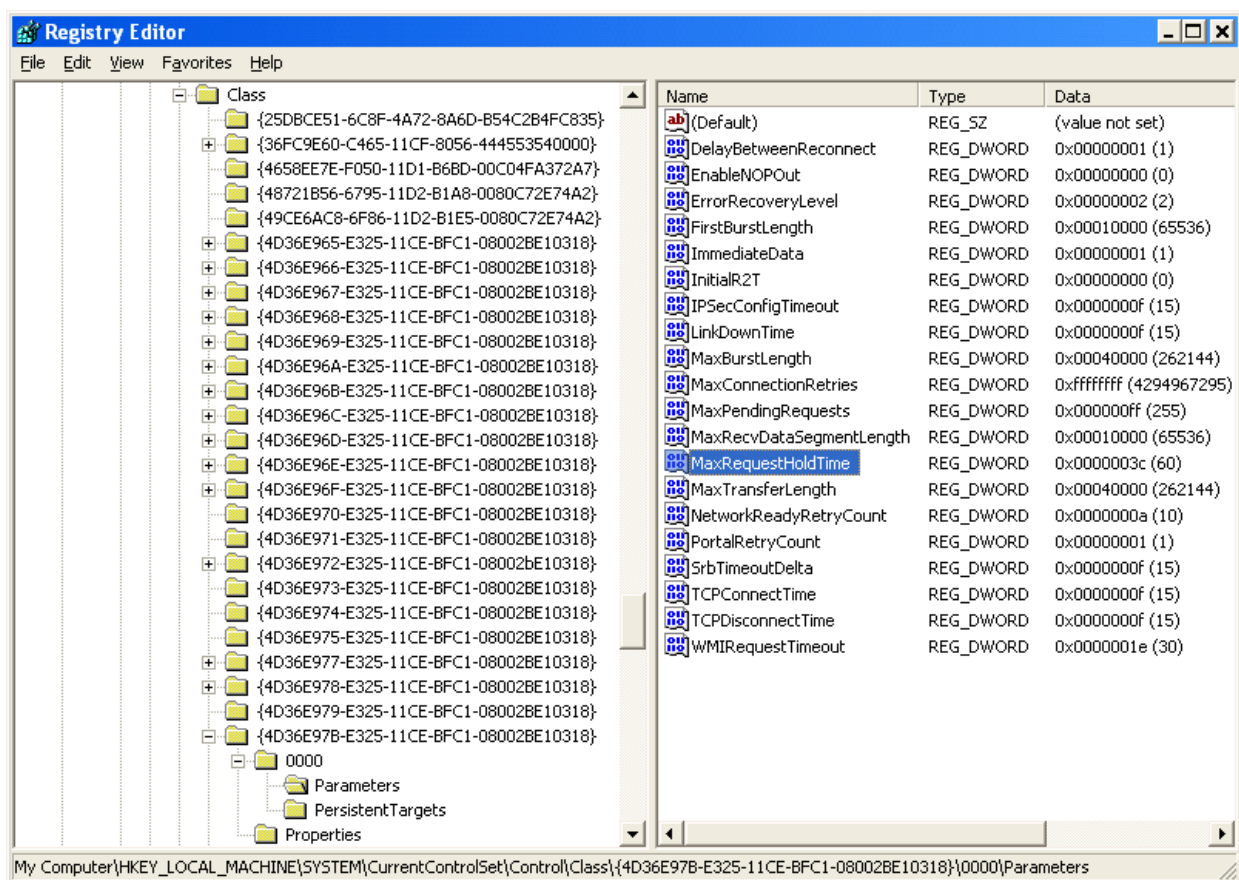
Setting the Session Timeout

The following procedure sets the MaxRequestHoldTime value to 10 minutes.

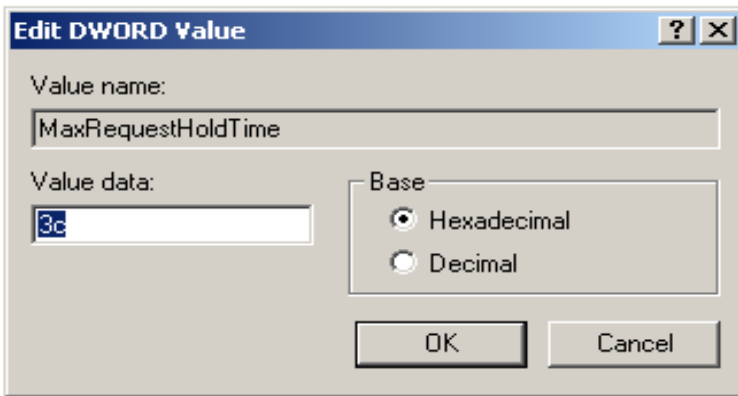


Take standard precautions when editing the registry. If you are not comfortable with this process, consider making a backup copy of the registry before starting. For more information on backing up, editing and restoring the registry, please refer to the following Microsoft Knowledge Base article: Description of the Microsoft Windows Registry <http://support.microsoft.com/default.aspx?scid=kb;en-us;256986>.

1. To start the registry editor in Windows, click on Start and select Run from the menu.
2. Type regedit in the available Open: field, and click on OK.
3. Navigate to the following registry key:
4. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
5. With CurrentControlSet selected, click on the Edit menu and select Find.
6. Type in MaxRequestHoldTime and select Find.



7. Double-click on the MaxRequestHoldTime registry value, highlighted above, to bring up the following window:



8. Change the Base from Hexadecimal to Decimal
9. Enter 600 for the Value data and click on OK. This sets the MaxRequestHoldTime to 600 seconds (i.e., 10 minutes).
10. Exit the registry editor.
11. Restart the server to complete the updated registry value.

Creating the MaxRequestHoldTime Value

The MaxRequestHoldTime setting can be added to the registry if it is currently not present.

1. To start the registry editor in Windows, click on Start and select Run from the menu.
2. Type regedit in the available Open: field, and click on OK.
3. Navigate to the following registry key:
4. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
5. Within CurrentControlSet, navigate to and expand \Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
6. Under the key described in step 4, locate and expand the instance that has the plus (+) sign next to it. In the example below, this would be instance 0000.
7. Click the + sign next to the expandable instance, then select the Parameters key. This will reveal a list of available values in the right pane of the window.
8. Right-click the Parameters key described above.
9. From the drop-down menu click New, then click DWORD Value.
10. A new value entry will appear on the right side of the screen. Name the new value MaxRequestHoldTime, then press Enter on your keyboard.
11. You have now created the MaxRequestHoldTime value. Go back to Step 6 of the previous section for instructions on entering the proper data in the new registry value.

Expanding a Windows Volume on the SAN

OVERVIEW

Often times storage administrators need to expand volumes on a Windows server. Whether company growth, new requirements or changes in infrastructure, administrators require a SAN solution flexible enough to accommodate their changing storage needs. This section details the necessary steps to grow a disk on Windows 2008. Growing a disk in the LeftHand SAN is a simple two-step process that can be performed while the volumes are still on-line and accessible to applications/users

Increasing the Volume Size via the CMC

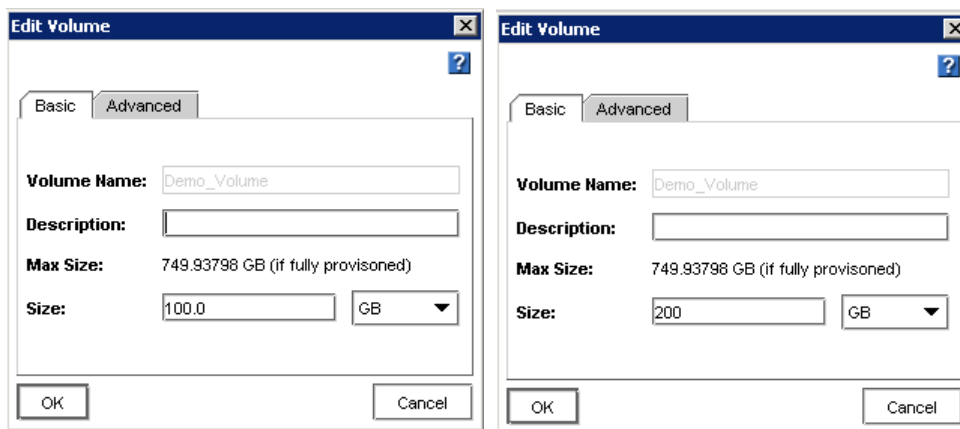
The first step in increasing the volume size is to increase the volume on the SAN so that it is large enough to meet your needs. Typically the size of the volume on the SAN and the size of the volume in Windows are designed to be the same. For this example, the 100 GB volume is being increased to 200 GB. This operation is completed via the Centralized Management Console and consists of the following steps:

1. Select the volume to increase in size
2. Double click to bring up the Edit Volume window
3. Adjust the volume size accordingly

Once the volume size has been increased on the SAN, steps must be performed in order for Windows to expand the partition to use the full space available on the disk.

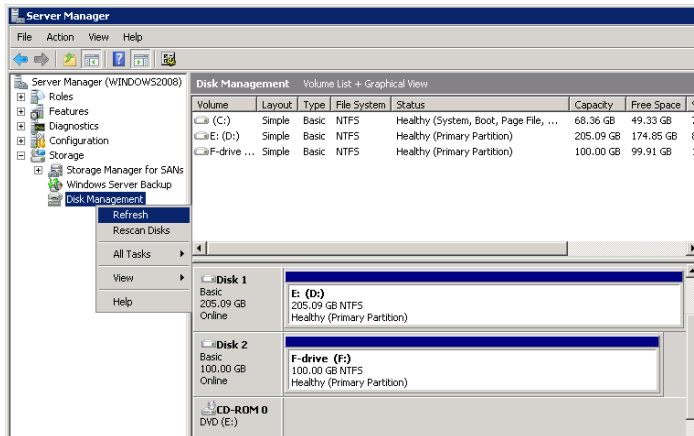
Increasing the Volume Size in Windows Via Disk Manager

1. Increase the volume on the SAN so that it is large enough to meet your needs. Typically the size of the volume on the SAN and the size of the volume in Windows are designed to be the same. For this example, the 100 GB volume is being increased to 200 GB.

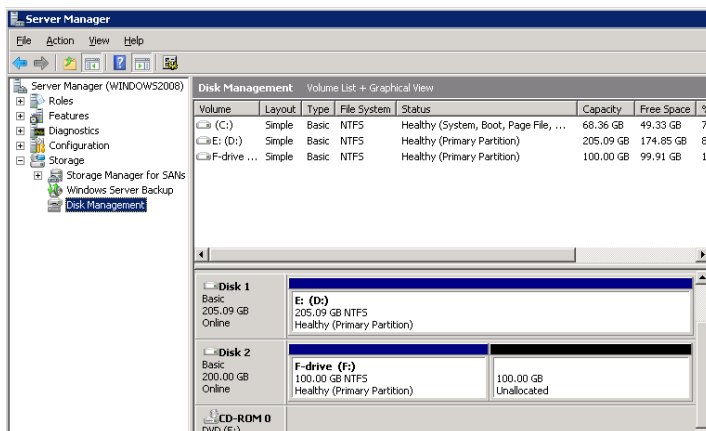


2. Go to Server Manager and open Disk Manager.

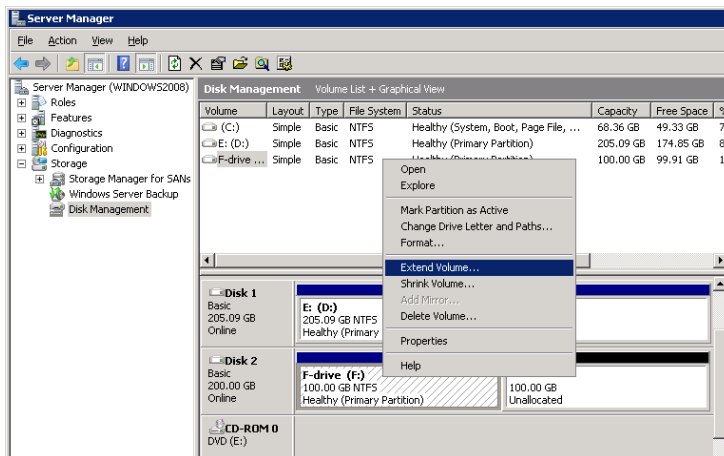
3. Refresh Disk Manager.



4. The additional space added in step one will appear next to the original volume.

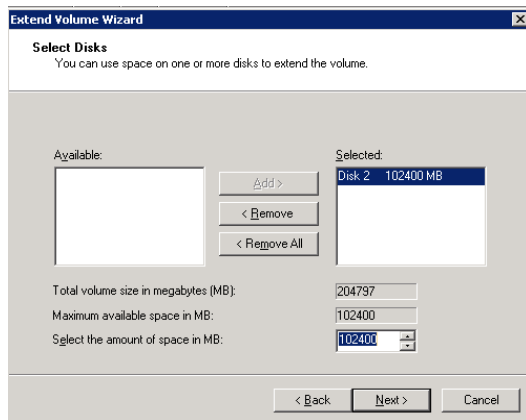


5. Right click on the volume you wish to extend (it must be on the same physical disk as the new free space), and click "Extend Volume"

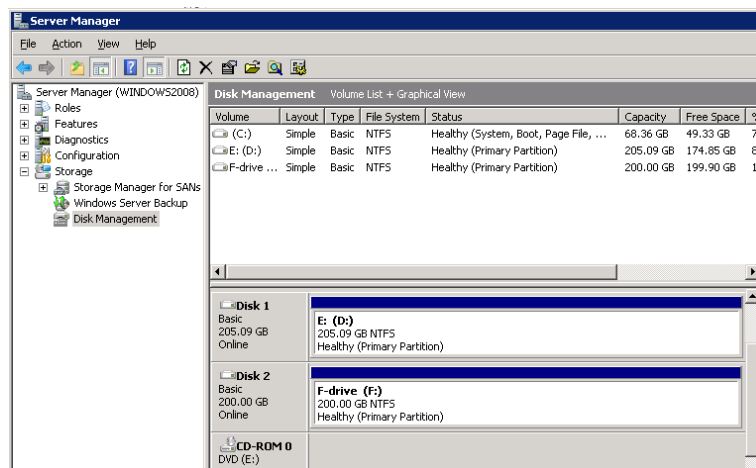


6. Extend Volume Wizard appears. Click Next.

- Choose the amount of space you wish to increase the volume by. The default amount is the maximum available space to add to the volume. Typically the volume on the SAN has been increased to the proper size, so choosing the default is usually correct. Click Next.



- A summary screen appears. If the summary looks correct, click Finish to begin the extension process.
- The volume now shows up with a new, larger, capacity.



Additional Documentation

Diskpart Command Reference <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/diskpart.mspx>

How to Use Diskpart.exe to Extend a Data Volume – describes how to use the Diskpart.exe command-line utility to extend a data volume into unallocated space. <http://support.microsoft.com/default.aspx?scid=kb;EN-US;325590>

The Partition Size is Extended, but the File System Remains the Original Size when you Extend an NTFS Volume <http://support.microsoft.com/default.aspx?scid=kb;EN-US;832316>

Shrinking a Windows Volume on the SAN

OVERVIEW

Occasionally, volumes are created and used on the SAN that end up being too large. SAN/iQ has Volume Shrink capability; however, in order to do this safely under a Windows NTFS file system, one must take careful steps in order to shrink the volume without data loss. There are several reasons why one may wish to shrink a volume:

Common Scenarios	Reason to Shrink
Volume simply too large	Sometimes, the estimates used to create the volume turn out to be too high. In these cases, one may want to retain the data on the volume, but simply make the volume smaller so that the space on the SAN can be used for other volumes.
Volume is no longer full	If the volume was full (or nearly full) and then space is freed up by users moving or deleting data off the volume, it would be ideal if one could simply shrink the volume to a size that is more in line with what is in use on the NTFS file system.
Volume is not a good candidate for thin provisioning* (Prior to SAN/iQ version 7.0 only. In SAN/iQ 7.0, simply convert the volume to Full Provisioning.)	Some volumes turn out to be poor candidates for a SAN/iQ Volume provisioning technique called Thin Provisioning*. In these cases, for SAN/iQ versions prior to 7.0, it is best to shrink the volume down to what is actually in use on the file system.
Project is cancelled; space is freed up	In most organizations, projects come and go. If a project is cancelled, or significantly scaled back, the storage needs for the project may be much less. In these cases, it makes sense to shrink the volume.
Application growth is slower than expected	Sometimes, the growth estimate for a volume turns out to be too high. If the data is not growing as fast as anticipated, it may be prudent to shrink the volume so that the space on the SAN can be better utilized by volumes that are growing more quickly.
Volumes created as Full Provisioned while using SAN/iQ versions earlier than 7.0 may not take advantage of the Thin Provisioning 2.0 features found in SAN/iQ 7.0.	Changing these volumes to Thin Provisioning in SAN/iQ 7.0 may not regain space as anticipated. For more information on Thin Provisioning, go to http://www.lefthandnetworks.com/thinprovisioining.aspx

Shrinking Volumes on the SAN

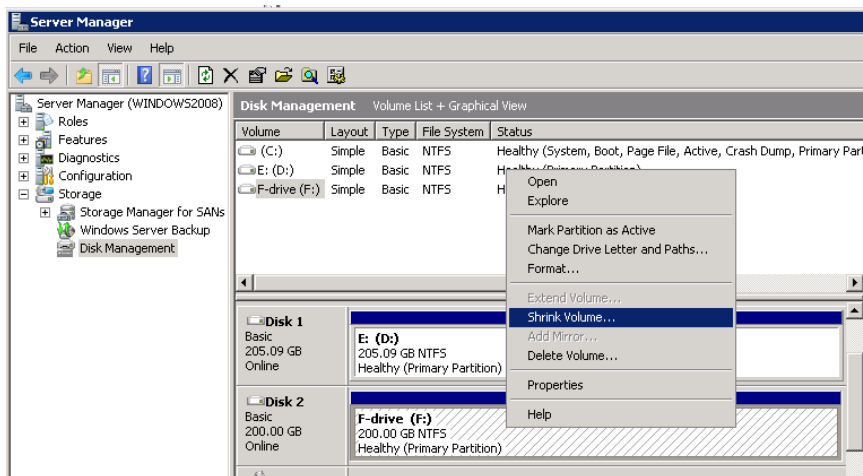
The capability to shrink volumes on a LeftHand Networks-powered SAN has been a product feature since the product was introduced. However, in order to shrink a volume on the SAN without destroying the data on the volume, one must perform the shrink steps in precise order. Performing the steps out of order can result in complete data loss on that particular volume. Shrinking volumes can be a tedious, time-consuming task. There may be other options that relieve the specific pain point you're addressing, such as doing a volume migration to a new cluster or, for volumes created while using SAN/iQ version 7.0, converting a worrisome volume from fully provisioned to thinly provisioned. Thin provisioning does not shrink the size of the volume that is presented to the host, but rather only allocates space on the SAN on an as-needed basis – meaning space on the SAN isn't used until data is actually written to the blocks.



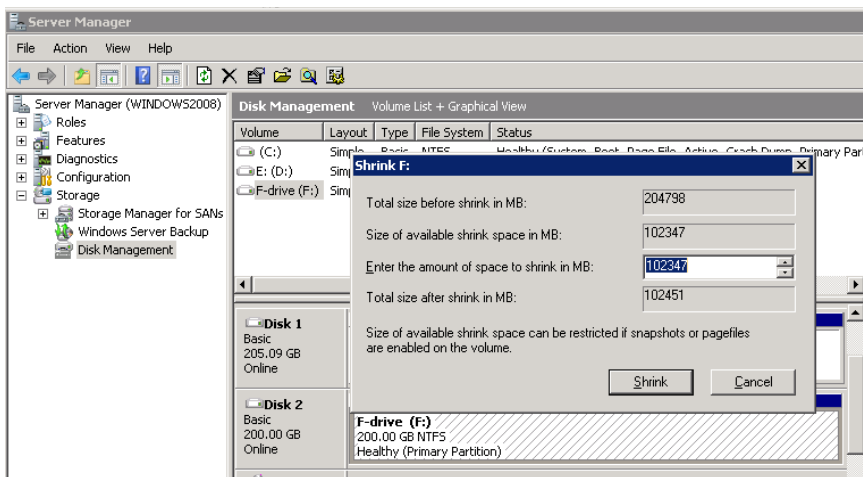
The NTFS file system must be shrunk before shrinking the SAN volume to prevent data loss.

The following example will walk through the process of shrinking a 200GB SAN Volume and NTFS file system down to 100GB.

1. Run CHKDSK against the NTFS file system.
2. Verify backups of the volume being shrunk.
3. Create a Snapshot of the Volume on the SAN. This provides a quick recovery option as well as a secondary backup copy of the volume.
4. Use Microsoft Disk Management to shrink the file system.

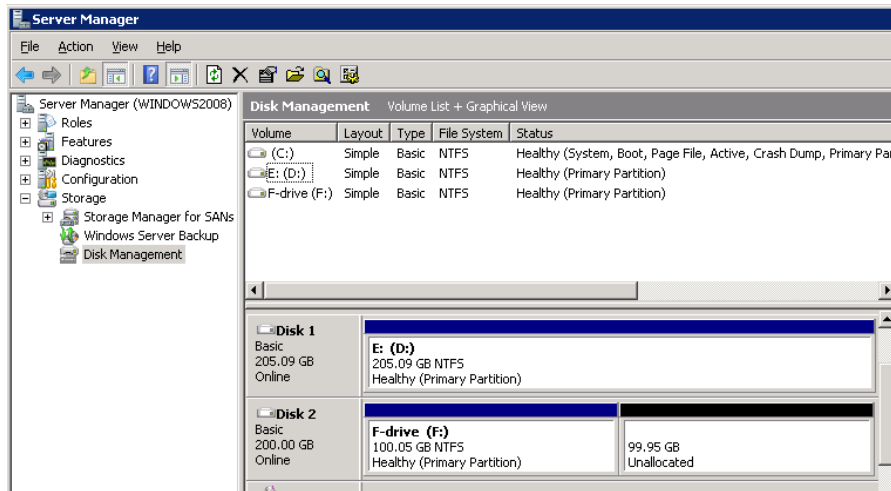


5. A dialog box pops up. The maximum available shrinkage amount is automatically calculated and displayed. Enter the amount of space you wish to shrink the volume by. In other words, how much space you wish to remove from the partition.

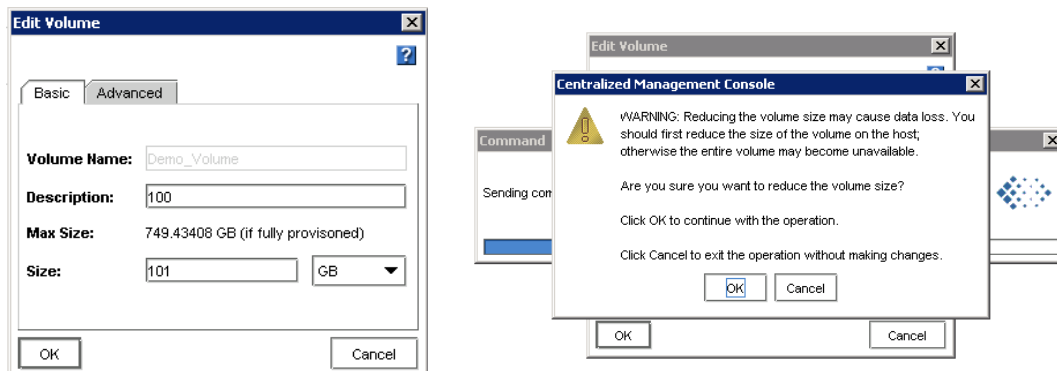


This procedure can take significant time to complete depending on how much data is in the file system.

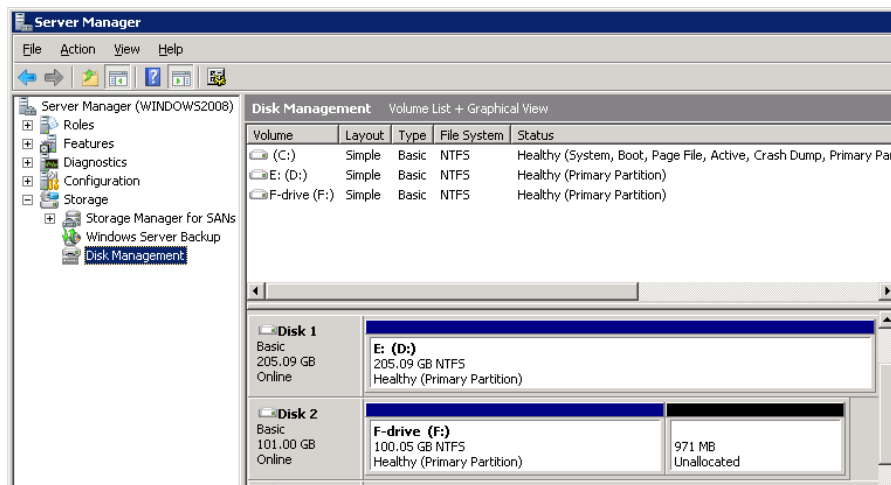
6. File System after being shrunk



- Shrink the volume on the SAN. Be sure that the volume on the SAN is as least as large as the volume on the server. Using the management console, edit the volume and set the new Size of the volume to be a small increment (50-100MB) greater than the new size of the file system. This is to ensure that the entire Windows volume will fit on the volume created on the SAN. If the volume on the SAN is smaller than the Windows volume, data loss can occur.



- This is a view of the new file system and volume size in Windows Disk Management. Note the small 'Unallocated' portion of the physical disk that remains after the shrink. This is the "buffer" from the previous step. You can choose to expand the volume to include this extra space if you wish.



9. Run CHKDSK against the NTFS file system.
10. Optionally delete the snapshot created in Step 3.

Shrinking Volumes on the SAN in Windows 2008 Server Core

1. Run CHKDSK against the NTFS file system.
2. Verify Backups.
3. Create a Snapshot of the Volume on the SAN.
4. Launch diskpart.exe by selecting Start > Run, type cmd in the Open box, click OK, then type diskpart.exe at the prompt.
5. Select the proper volume (Volume 3 in this example)

```
select volume 3
```

6. You can determine the maximum amount of space available to shrink by using the following command:

```
shrink querymax
```

7. To perform a shrink to a certain amount, add the desired parameter with the number of megabytes by which to shrink. You can also add a minimum parameter, which forces the command to fail if that amount of space isn't available. You can use a combination of parameters. So, if you specify "desired=100000 minimum=50000," the tool will attempt to shrink by 100 GB, but as long as it can shrink by at least 50 GB, the command will execute successfully. For example:

```
shrink minimum=20000
```

8. Complete the shrink process on the SAN as detailed in steps 7 – 10 above.



Microsoft counts 1 GB as 1024 MB. Shrinking a volume by 100,000 MB is not the same as shrinking it by 100GB. This difference is reflected in the screenshot below, where the volume was shrunk by 98 GB (100,000 / 1024 = 98 GB). This is especially important when shrinking the volume on the SAN because if 100 GB is specified in the management console, the volume would be shrunk by 100 GB and the new size would be 2 GB smaller than what the OS is expecting to see.

```
Administrator: C:\Windows\system32\cmd.exe - diskpart

DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> list volume

Volume ### Ltr Label      Fs      Type        Size      Status      Info
-----
Volume 0    E             NTFS     DVD-ROM      0 B        No Media
Volume 1    C             NTFS     Partition    68 GB      Healthy     System
Volume 2    D  E:         NTFS     Partition    205 GB     Healthy
Volume 3    F  F-Drive    NTFS     Partition    200 GB     Healthy

DISKPART> select volume 3
Volume 3 is the selected volume.
DISKPART> shrink minimum=100000
DiskPart successfully shrunk the volume by:  98 GB
DISKPART> list volume

Volume ### Ltr Label      Fs      Type        Size      Status      Info
-----
Volume 0    E             NTFS     DVD-ROM      0 B        No Media
Volume 1    C             NTFS     Partition    68 GB      Healthy     System
* Volume 2    D  E:         NTFS     Partition    205 GB     Healthy
* Volume 3    F  F-Drive    NTFS     Partition    102 GB     Healthy

DISKPART> _
```

Measuring Performance in a Windows Environment

OVERVIEW

This section describes how to use Perfmon to measure performance on a Windows system connected to a volume on the SAN.

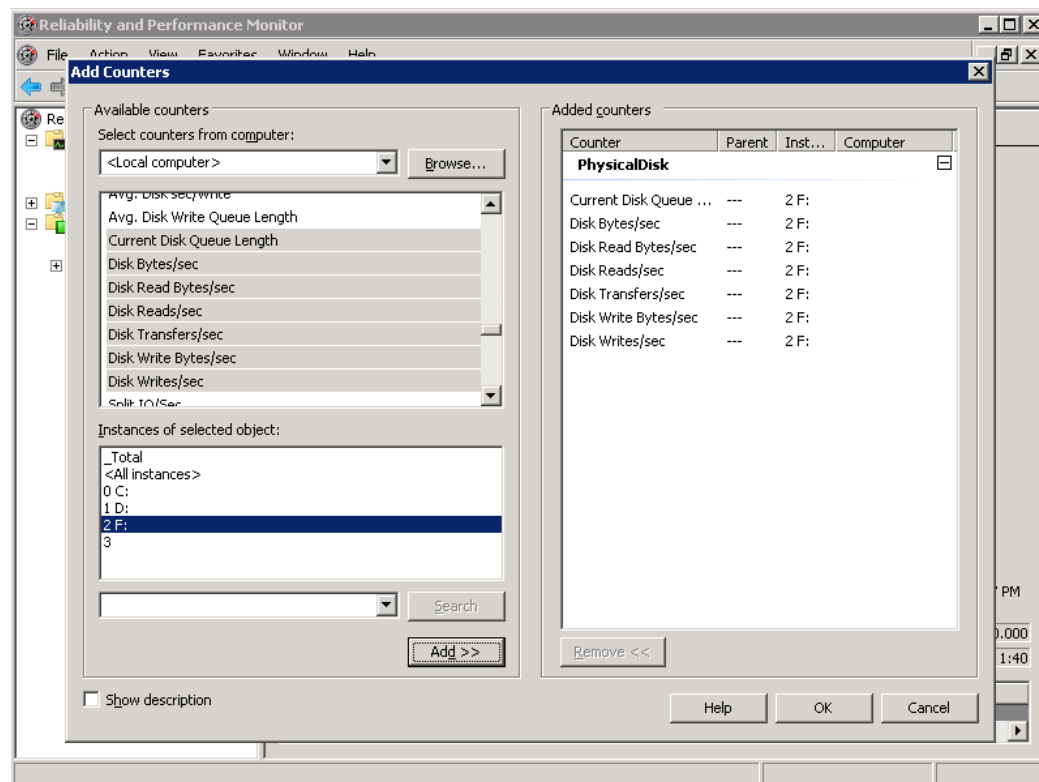
Using Windows Performance Monitor to Measure SAN Performance

The preferred method to measure application server performance connected to the SAN is to use Windows Performance Monitor (perfmon.exe) and sample the appropriate PhysicalDisk counters for the SAN volume(s) in question. The following are relevant performance counters and what they measure:

Performance Counter	SAN Measurement	Notes
Avg. Disk Sec/Read	Read I/O Latency of the volume	Measured in Seconds. Typical values are in milliseconds.
Avg. Disk Sec/Transfer	I/O (Read & Write) Latency of the volume	Measured in Seconds. Typical values are in milliseconds.
Avg. Disk Sec/Write	Write I/O Latency of the volume	Measured in Seconds. Typical values are in milliseconds.
Avg. Disk Queue Length	Average # of pending I/O requests for the volume	Measured as the raw number.
Current Disk Queue Length	Current # of pending I/O requests for the volume	Measured as the raw number.
Disk Bytes/sec	Total data throughput for the volume	Measured in Bytes/sec. Typical values are in Megabytes/sec.
Disk Read Bytes/sec	Read data throughput for the volume	Measured in Bytes/sec. Typical values are in Megabytes/sec.
Disk Write Bytes/sec	Write data throughput for the volume	Measured in Bytes/sec. Typical values are in Megabytes/sec.
Disk Reads/sec	Read IOPS (I/Os / sec) for the volume	Measured as the raw number.
Disk Writes/sec	Write IOPS (I/Os / sec) for the volume	Measured as the raw number.
Disk Transfers/sec	Total IOPS (I/Os / sec) for the volume	Measured as the raw number.

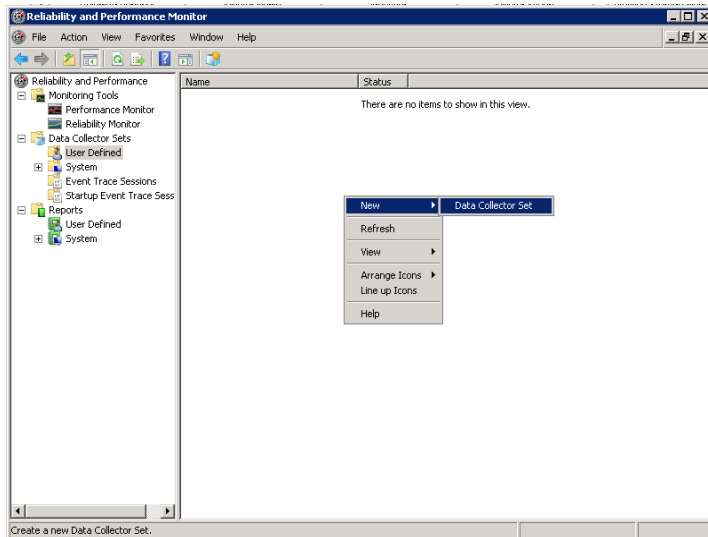
Setting up Windows Performance Monitor

1. Open Windows Performance Monitor (Start Menu>Accessories>System Tools>Performance Monitor, or run the perfmon.exe program).
2. Click the X icon several times to remove any existing counters.
3. Click the + icon or right-click on the graph area to open the Add Counters function.
4. Configure the Add Counters window as shown below. Make sure to include all counters listed above. (To simplify the process, choose “All counters” from the column on the left to avoid having to individually select counters). Add the PhysicalDisk counters listed in the table above, and then click the Add button
5. Make sure to choose the proper physical disks from the section on the right. Unless directed to do otherwise, select all disk instances and do not choose the _Total. Selecting all the individual disks allows for a more detailed analysis of the performance data.
6. Select Close. *Choosing the “view report” icon rather than the “view graph” icon will generally reveal more useable results.

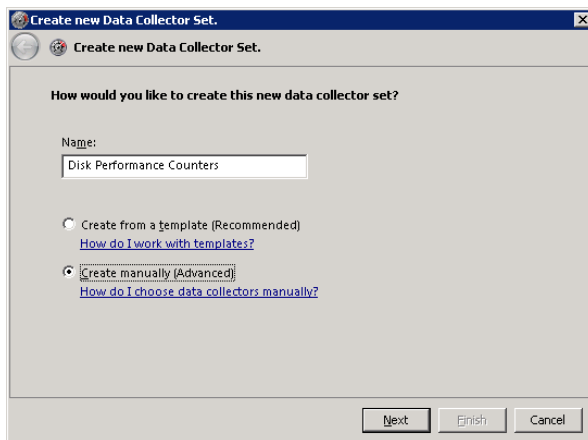


Saving A Performance Monitor Log for Analysis

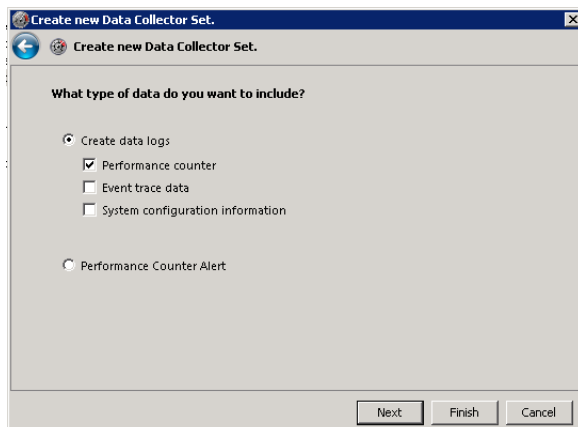
It is common for Administrators to monitor performance on a longer-run basis. If needed, setup a performance counter log by expanding Performance Logs and Alerts, right-click Counter Logs, and select New Log Settings.



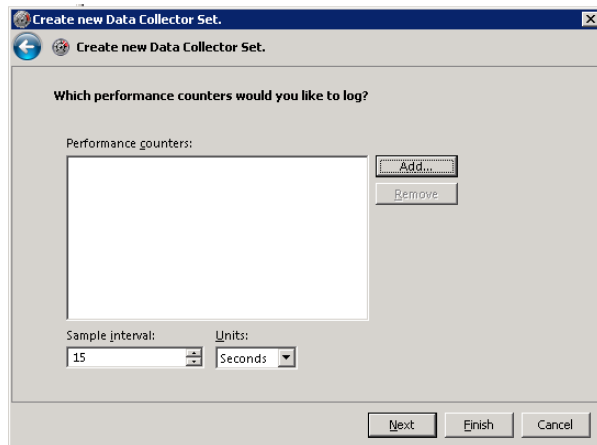
Provide a meaningful name and choose to manually create the data collector set.



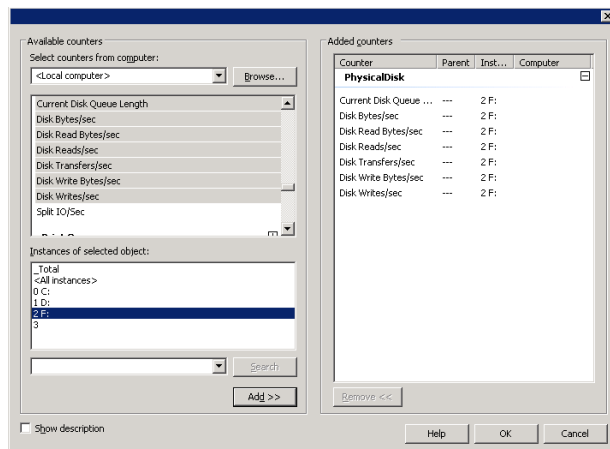
Choose to create a data log of Performance counters.



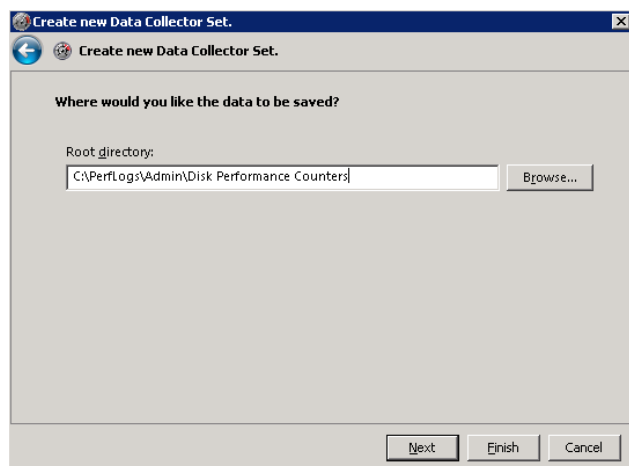
Click “Add...” to add counters to the collection set. The sample interval (rate) can also be changed here. The default of 15 seconds is usually suggested.



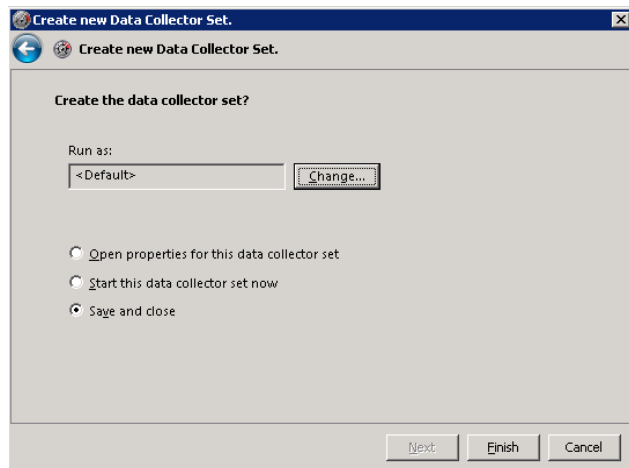
Choose the counters that you wish to add. If unsure, choose all physical disk counters and all instances.



Choose where the data (logs) are to be saved. It is a good idea to save the logs to a location that is not being monitored for performance, as to minimize the effect of the logging itself on the data.



Choose to save and close the Data Collector Set.

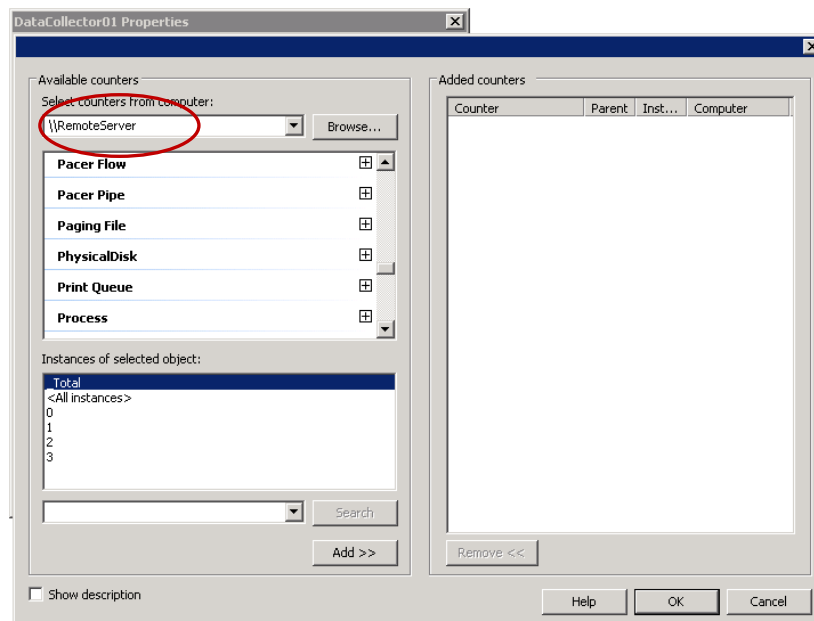


NOTES:

- The output file can be saved as a binary log (blg) or a comma-separated file (csv). To change the output format, select the Log Files tab. The .blg format file can be viewed later in Performance Monitor. The .csv file can be imported into a spreadsheet or database for further analysis.

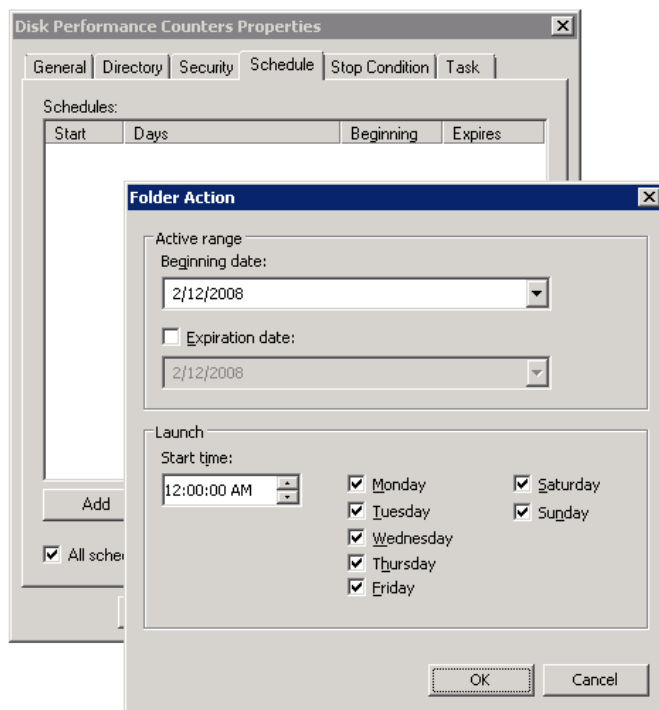
Monitoring more than one server simultaneously

When collecting data from multiple servers, you can collect all data from a single perfmon instance by changing the server name in the “Select counters from computer:” box. The appropriate physical drives will show up for that server. For example, a remote server that is running SQL Server would have specific SQL Server counters appear, even though the server doing the monitoring does not have SQL Server installed.

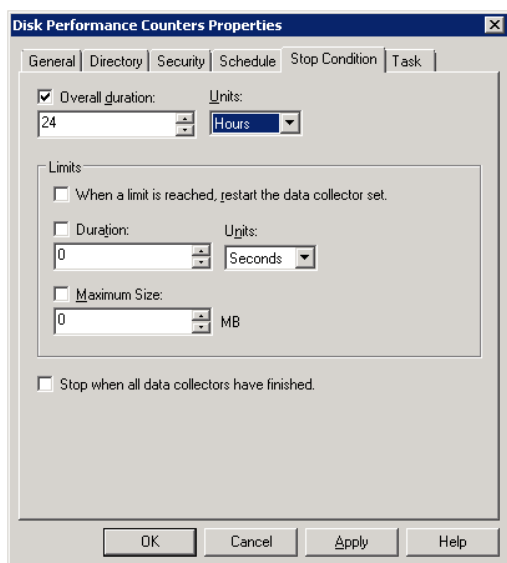


Scheduling performance data collection

Data collection can be scheduled using the Performance Monitor tool. To enable scheduling, right-click on a log that has been created, and select “Properties”. Go to the “Schedule” tab to set up the start and stop time for the performance data logging. The most value comes from a schedule that encompasses typical workloads, so it is suggested that the schedule be set to include times with peak loads, such as backups, end-of-week batch processing jobs, or other times when the SAN is heavily utilized. Depending on the individual environment, this schedule could last for 24 hours to one week. Typically, logging of less than 24 hours does not represent a comprehensive workload.



Go to the Stop Condition tab to define a duration for the test to run. Typically data that is less than 24 hours in duration is less useful. Typically 72 hours provides the best combination of useful information and manageable data. It is important that peak workloads occur during the time period that the data collection is occurring.



USING IOMETER AS A SAN BENCHMARK TOOL

IOMeter is a performance benchmark application that can generate customizable I/O loads against disk devices to measure performance. IOMeter is an Open Source software package contributed by Intel to the Open Source Development Lab. The OSDL and individuals within the community now maintain the package. As the IOMeter User's Guide says, IOMeter is an I/O subsystem measurement and characterization tool for single and clustered systems.

The software is available from <http://www.IOMeter.org/> or <http://sourceforge.net/projects/IOMeter/>. Download and install the Win32 version of IOMeter on the Windows server that will be used to generate the I/O load.

Configuring the iSCSI Volume

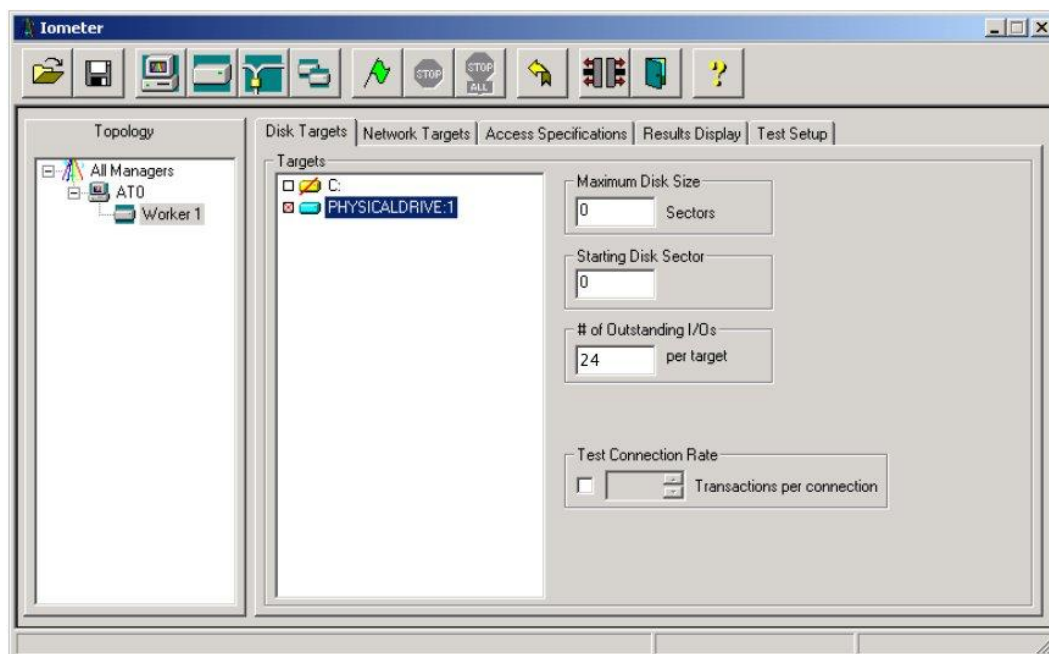
Using the SAN/iQ Management Console, create a volume with the size and thresholds all set to the same amount, e.g. 10GB. Set Replication Levels and other parameters to appropriate values. Apply a read-write Volume List to the volume and configure an Authentication Group for the application server, then use the iSCSI Control Panel to add the test volume.

Optionally, launch Windows Performance Monitor and setup the counters according to the section above.

Configuring IOMeter

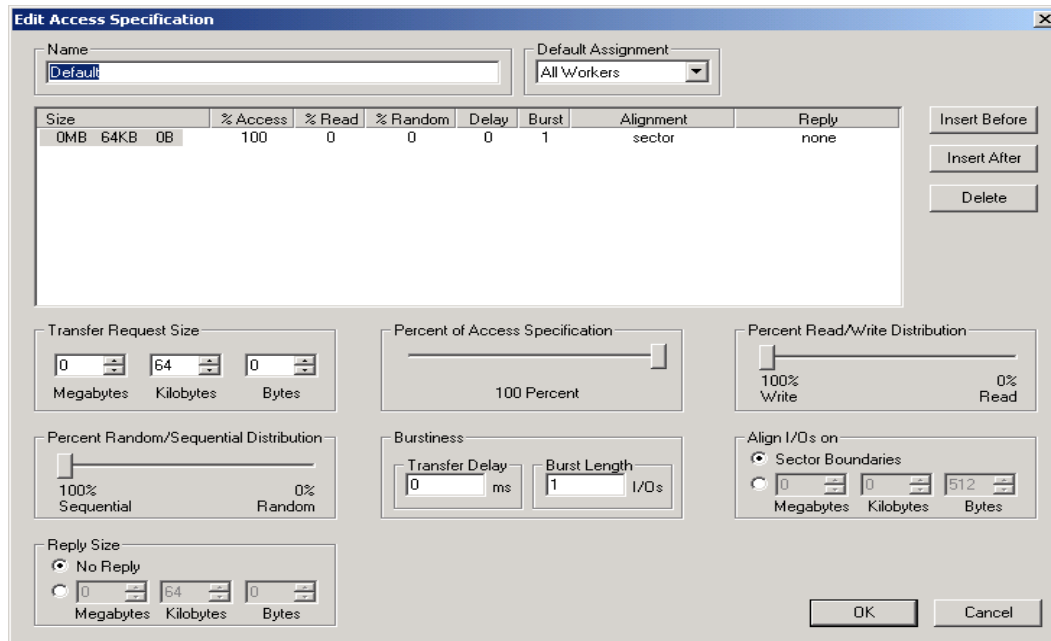
Start IOMeter and the main window will come up. Below the Topology pane will be the local server name with a Worker below it. If you have a multi-processor Windows Server, you will see a Worker for each processor.

Highlight the first worker in the list, and then select the drive number of the raw disk which was created for the test. Enter a number into the “# of Outstanding I/Os per target” that is equal to two times the amount of individual disk drives in your SAN cluster. For example, three NSM-160s have four disks each times the three NSMs equals twelve disks. So, twenty-four would be used for the “# of Outstanding I/Os”.



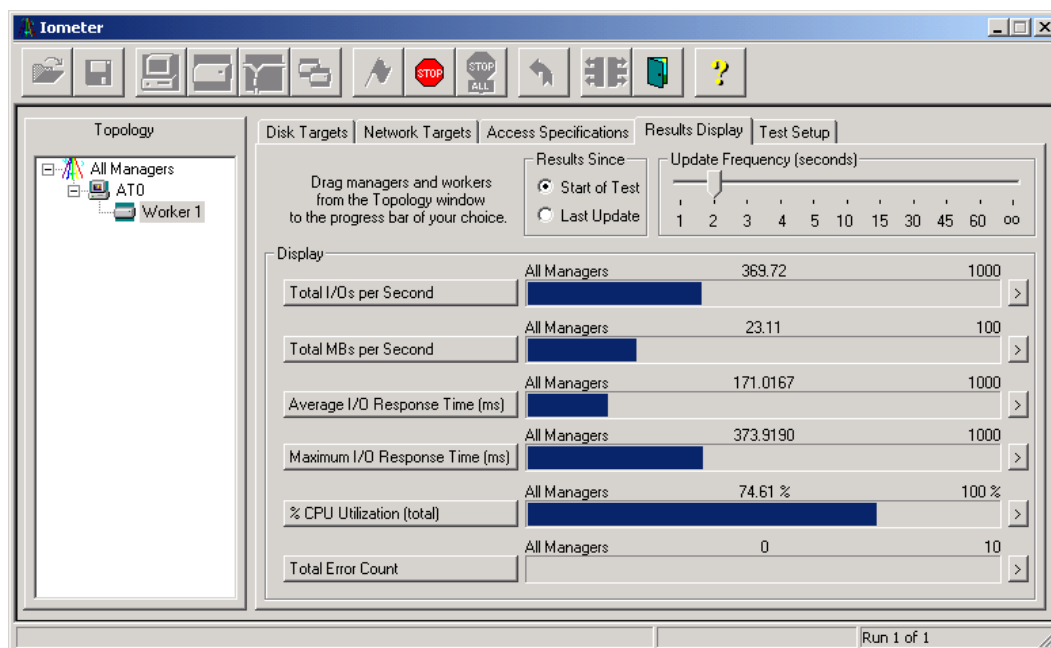
Configuring IOMeter Access Specification for each test

Select the Access Specifications Tab. Highlight the Default access specification profile under the Global Access Specifications column on the far right of the screen. Click on Edit. A new window will be invoked titled “Edit Access Specification”. Set the “Transfer Request Size”, “Percent Random/Sequential Distribution”, and the “Percent Read/Write Distribution” with the values in the chart at the end of this document. Leave the other parameters at their default settings. Hit “OK” to save the Access Specification and return to the main IOMeter window.



Running the Test

Click the Green Flag on the top button bar to start the test. Select the “Results Display” tab in the IOMeter window. Drag the slider under “Update Frequency (seconds)” over to 1 or 2 seconds.



Interpreting Results

Use the Windows Performance Monitor to validate the results that IOMeter reports. By default, IOMeter reports in Megabytes per second and the Windows Performance Monitor reports in Bytes per second. To convert the IOMeter MB/sec to Bytes/sec, multiply by 1024 and then again by 1024.

Access Specifications to Run

Run the following access specifications to emulate different use scenarios and record your results. The typical results listed below were run on a Windows 2003 Server with Service Pack 2. The SAN was running SAN/iQ 7.0 with VIP load balancing enabled (no DSM). The switches had flow control enabled, but jumbo frames were not.

Transfer Request Size	Percent Random/ Sequential Distribution	Percent Read/Write Distribution	Why this specification matters	Typical results for 3 DL320s SAS in RAID 5 with 2 way replication		Your test results	
64K	50% Random	50% Write 50% Read	This specification is similar to a heavily used file share	MB/s	IOPS	MB/s	IOPS
				38	600		
4K	100% Random	20% Write 80% Read	This specification is similar to a Microsoft Exchange Database	MB/s	IOPS	MB/s	IOPS
				23	6000		
8K	100% Random	33% Write 67% Read	This specification is similar to a Transactional Database	MB/s	IOPS	MB/s	IOPS
				33	4200		
4K	100% Sequential	100% Write	This specification is similar to a Microsoft Exchange log files	MB/s	IOPS	MB/s	IOPS
				34	8700		
64 K	100% Sequential	100% Read	This specification is similar to a backup of data from the ISCSI SAN	MB/s	IOPS	MB/s	IOPS
				110	1700		

Frequently Asked Questions

The following FAQ covers majority of the questions related to customers using the new Microsoft iSCSI initiator within a LeftHand SAN.

Microsoft Windows 2008 Server

Q: What versions of SAN/iQ are supported with Microsoft Windows 2008 Server?

A: The only versions of SAN/iQ that are supported with Microsoft Windows 2008 Server are versions 7.0 and higher. For the most current list of supported software, download the LeftHand Compatibility Matrix from the Resource Center (https://www.lefthandnetworks.com/member_area/dl_file.php?fid=554&action=display)

Q: Does the new Windows 2008 support Dynamic Disks over iSCSI?

A: Dynamic Disks are now supported with Windows 2008. Refer to section 2 above for more details.

Q: Does Windows 2008 support booting from a LeftHand SAN?

A: Yes.

Microsoft MPIO

Q: Should customers use the Microsoft MPIO with the new iSCSI initiator?

A: The only supported method for using Microsoft MPIO framework is in conjunction with the LeftHand Networks DSM for MPIO. The LeftHand DSM for MPIO will be available as part of the LeftHand Networks' Windows Solution Pack, available from your reseller. For more information on the Windows Solution Pack and availability, contact your VAR or LeftHand Networks.

Q: Do I need to uninstall the MPIO that comes standard with Windows 2008?

A: No. Leaving MPIO installed does influence the iSCSI connection to your LeftHand SAN. However, DO NOT modify the MPIO settings through the MPIO control panel, and DO NOT enable multi-path when logging on to a volume.

LeftHand Networks' Windows Solution Pack

Q: Will I be able to use VSS/VDS/DSM from my current Windows Solution Pack?

A: There will be a version of the Windows Solution Pack which will be supported for Windows 2008. Versions of the Windows Solution Pack prior to this release will not be supported for Windows 2008. If a previous version of the Windows Solution Pack is installed on a server running Windows 2008, it must be uninstalled. When the new Windows 2008 solution pack becomes available, customers who have purchased the Windows Solution Pack and who have an active support contract will be given a free upgrade.

Appendix A: Changes for Windows 2008

Windows 2008 Server Core:

Windows 2008 Server Core is a much-scaled back version of Windows 2008 Server. What makes Core stand out is that it is a stripped down, lean version of the Windows 2008 operating system. Most interaction with Windows 2008 Server Core is via the command line interface (CLI), as familiar tools such as Explorer and the Windows desktop are not installed with Server Core. A Server Core installation is defined by its role, a predefined set of applications that when installed and configured, allow the server to perform certain functionality. For example, a server with the role of Web Server would have IIS, etc. installed and configured.

Because the interface to Server Core is so unlike other versions of Windows, special attention was given to interacting with Server Core in this document.

iSCSI Initiator:

The iSCSI initiator now comes built in to all Windows 2008 Server versions. It no longer needs to be downloaded and installed as a separate piece of software. Updates to the iSCSI initiator are now done through Windows Update.

Persistent Targets are now referred to as Favorite Targets.

MPIO and DSM:

Microsoft's MPIO and DSM are not supported with SAN/iQ.

Managing Partitions in Windows 2008:

Dynamic Disks over iSCSI are now supported in Windows 2008. This is a change from previous versions of Windows Server.

Users can extend or shrink volumes from the Disk Management GUI. A wizard exists for both operations. Previous versions of Windows Server required using diskpart or diskpar to extend the partitions, and a third party application to shrink partitions.

Partitions created in the Disk Management GUI are now offset by default (refer to Section 2 of this document). The amount of the alignment is dictated by the size of the volume. The values for the offset can be controlled by editing the registry keys at HKLM\System\CurrentControlSet\Services\VDS\Alignment. Previous versions of Windows Server had no offset by default. Diskpart or diskpar was required to create a partition with an offset.

Appendix B: Commonly Used Commands for Setting up and Configuring a Windows 2008 Core Server

To set a static IP address:

1. At a command prompt, type the following:

```
netsh interface ipv4 show interfaces
```

2. Make a note of the number shown in the Idx column of the output for your network adapter. If your computer has more than one network adapter, make a note of the number corresponding to the network adapter for which you wish to set a static IP address. Then, at the command prompt, type:

```
netsh interface ipv4 set address name="<ID>" source=static  
address=<StaticIP> mask=<SubnetMask> gateway=<DefaultGateway>
```

ID is the number from step 1 above

StaticIP is the static IP address that you are setting

SubnetMask is the subnet mask for the IP address

DefaultGateway is the default gateway

3. If the network adapter is on a private network for iSCSI traffic, a DNS server is not required for that network adapter. For reference however, to add a DNS Server to the network adapter configuration, at the command prompt, type:

```
netsh interface ipv4 add dnsserver name="<ID>" address=<DNSIP>index=1
```

ID is the number from step 1 above

DNSIP is the IP address of your DNS server

4. Repeat step 4 for each DNS server that you want to set, incrementing the index= number each time. If you set the static IP address on the wrong network adapter, you can change back to using the DHCP address supplied by using the following command:

```
netsh interface ipv4 set address name="<ID>" source=dhcp
```

ID is the number of the network adapter from Step 1.

To configure the firewall to allow Remote Administration of the server:

Use the netsh advfirewall command. For example, to enable remote management from any MMC snap-in, type the following:

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

To enable remote desktop connections (RDP):

To allow Remote Desktop connections to the Windows 2008 Core Server, type the following from the command prompt:

```
cscript C:\Windows\System32\Scregedit.wsf /ar 0
```

You can also use the Windows Firewall snap-in from a computer running Windows Vista or Windows Server 2008 to remotely manage the firewall on a server running a Server Core installation. To do this, you must first enable remote management of the firewall (see above)

Configuring the iSCSI Initiator:

The first time a Windows 2008 Server Core system is connected to a LeftHand SAN, the Microsoft iSCSI service must be started. To do this, type the following at the command prompt:

```
sc start msiscsi
```

To have the service start automatically on boot, type the following at the command prompt:

```
sc config msiscsi start= auto
```

To check the status of the iSCSI Initiator Service, type the following at the command prompt:

```
sc interrogate msiscsi
```

Additional Resources:

Server Core Installation Option of Windows Server 2008 Step-By-Step Guide –

<http://technet2.microsoft.com/windowsserver2008/en/library/47a23a74-e13c-46de-8d30-ad0afb1eaffc1033.mspx?mfr=true>

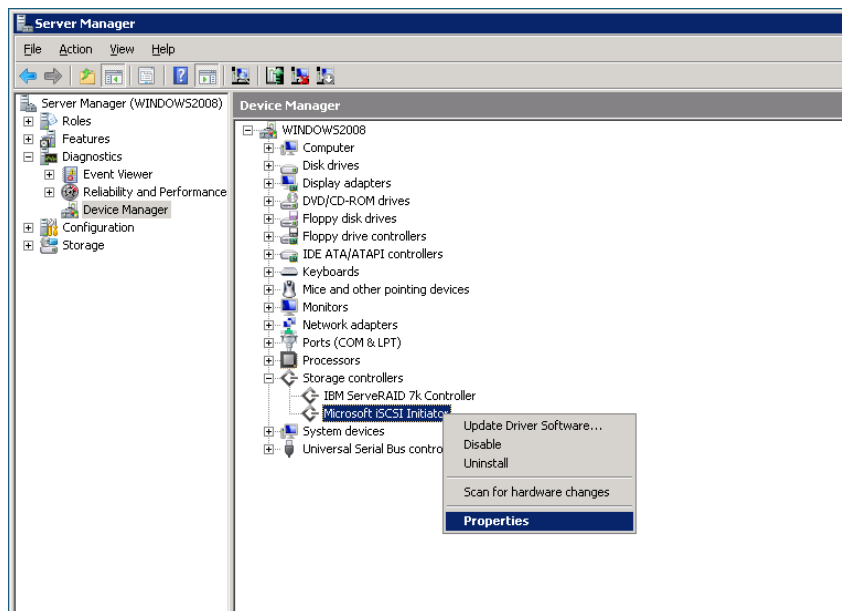
Appendix C: Finding the iSCSI Initiator Version

OVERVIEW

This section provides instructions on how to determine the version of Microsoft iSCSI initiator being used. When calling LeftHand Networks support, or troubleshooting iSCSI issues, it is helpful to know what version of the Microsoft iSCSI initiator you are using.

Using The Windows Device Manager to Determine iSCSI Initiator Version

Open the Device Manager by right-clicking My Computer and selecting Manage. Select Device Manager in the Diagnostics section. In the System Properties window, select the Hardware tab and click Device Manager. The Device Manager Window opens.



In the Device Manager window, expand the SCSI and RAID Controllers section and double-click the Microsoft iSCSI Initiator icon. The Microsoft iSCSI Initiator Properties window opens.

In the Microsoft iSCSI Initiator Properties window, select the Driver tab, and click “Driver Details...” The Driver File Details window opens.

Select the msiscsi.sys file and note the build number.

