

# Configuring Microsoft iSCSI Software Target in a Microsoft cluster



Introduction .....	2
Requirements .....	3
Prerequisites .....	3
Preparing cluster nodes .....	3
Configuring cluster nodes .....	4
Confirm resources failover .....	6
Configuring Microsoft iSCSI Software Target .....	7
Creating the iSCSI Target entry .....	7
Exporting an iSCSI virtual disk .....	9
Connecting to Microsoft iSCSI Software Target .....	11
Configuring advanced features .....	12
For more information .....	14

## Introduction

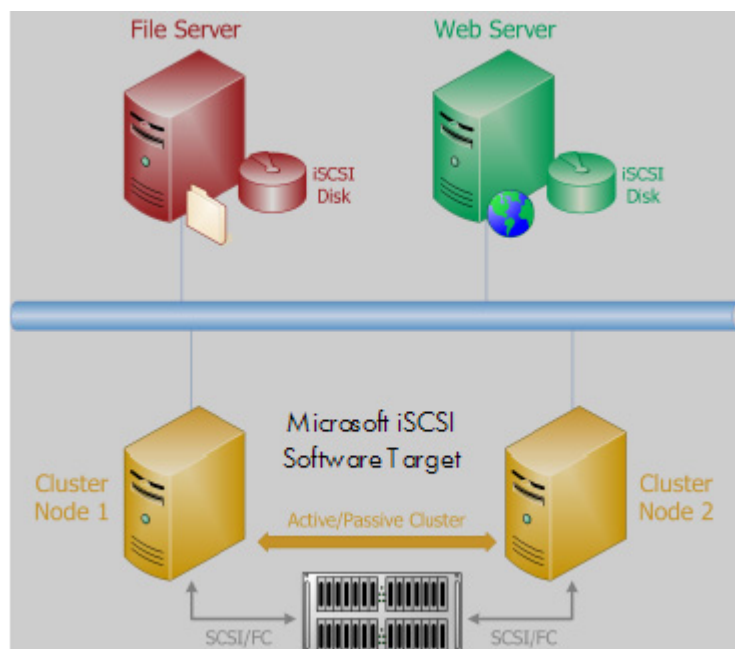
Redundant Array of Independent Disks (RAID) is a widely-adopted control framework for aggregating the capacity and performance of hard disk drives, while also providing fault tolerance. When a hard disk failure occurs, data flow continues, uninterrupted, by deriving information from the remaining disks in the array. For environments that have direct-attached RAID, applications (clients) using the storage reside on the same computer; therefore, protecting only the disk devices is sufficient.

In the consolidated storage model, the client that uses the storage no longer resides on the same computer, but rather on other computers on the network. The failure of the storage server in this environment has a much broader impact. To protect this storage resource, redundancy must now include other components of the system beyond the storage devices. Protecting the most vulnerable of these components (such as having multiple power supplies and NICs) is sufficient in most Small and Medium Business (SMB) environments; however, there are still some hardware components that cannot be made redundant.

To minimize the disruption window further, users can use software clustering. Software clustering is the ability to configure multiple servers to work as a single unit. Clustering protects the storage system from the unlikely event of failures caused by unprotected hardware. In this configuration, the failure of one server does not lead to total system outage. Instead, when one server fails, the workload shifts to the second server in the cluster, and work proceeds as normal.

Cluster environments that use external SCSI or Fibre Channel (FC) storage arrays that have built-in redundancy (multiple disk controllers, power supply, and so on) are expensive. Due to its high cost, this storage is reserved for the small number of highly critical clients. Administrators can maximize the usage of this redundant storage resource at a much lower per-client cost and achieve virtually continuous uptime by leveraging the functionalities of Microsoft® Cluster Service (MSCS) and Microsoft iSCSI Software Target. This document details the steps to configure Microsoft iSCSI Software Target for high availability using MSCS. The current release of Microsoft iSCSI Software Target only supports two-node clusters in an active/passive configuration.

Figure 1. Microsoft iSCSI Software Target and MSCS provide redundancy for iSCSI disks.



## Requirements

- Microsoft iSCSI Software Target
- Windows® Storage Server 2003 R2 or Windows Unified Data Storage Server 2003
- Microsoft iSCSI Software Initiator

## Prerequisites

- MSCS configured and running on the two nodes
- Sufficient free space on the shared disk to create Microsoft iSCSI Software Target Disk(s)

---

### Note

Throughout the rest of this document, the Windows cluster machines will be referred to as Node 1 and Node 2. The shared-disk resource to be used for creating Microsoft iSCSI Software Target disks will be referred to as E:\. Also, have the full name or IP address of the cluster available.

---

## Preparing cluster nodes

1. Use the Microsoft iSCSI Software Target installation wizard to Install Microsoft iSCSI Software Target on both nodes.

---

### Note

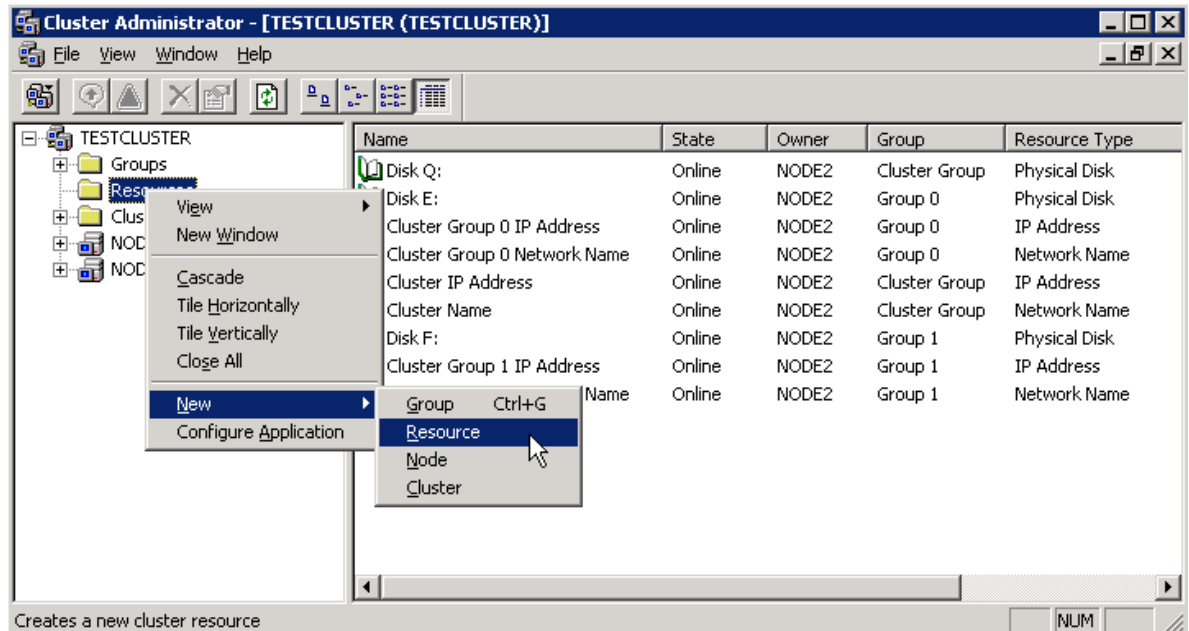
If you are running Microsoft Unified Data Storage Server 2003 on the cluster nodes, Microsoft iSCSI Software Target is preinstalled.

---

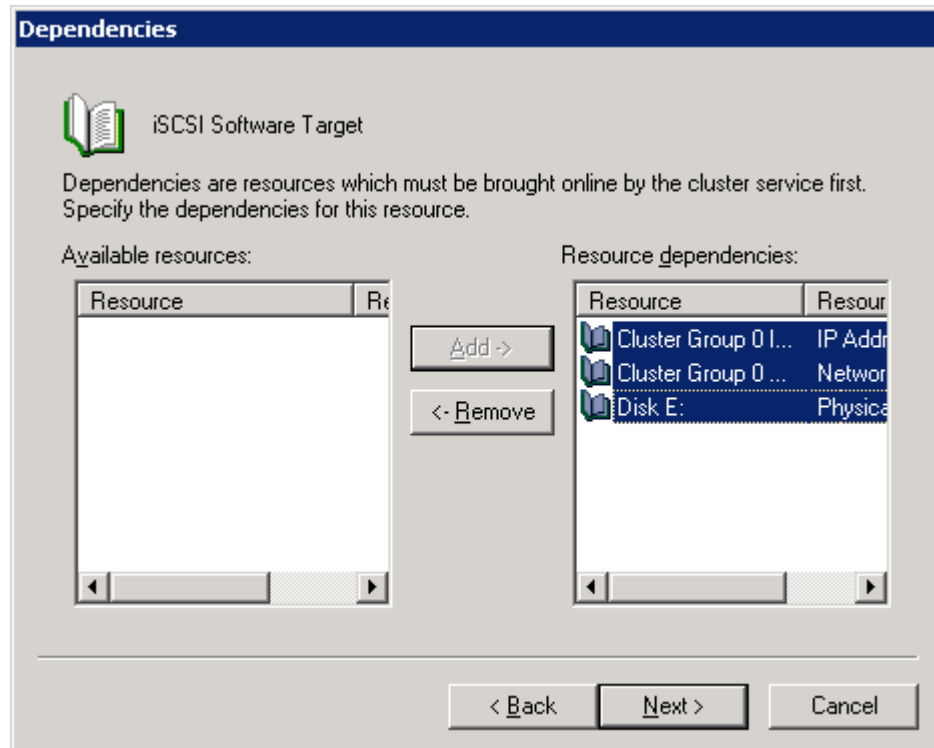
2. Uncheck the **Launch Microsoft iSCSI Software Target** check box on the final page of the wizard so that the iSCSI Target Console does not open when the installation is complete.
3. Stop the Microsoft iSCSI Software Target service by issuing **net stop wintarget** on the command line on both cluster nodes.

## Configuring cluster nodes

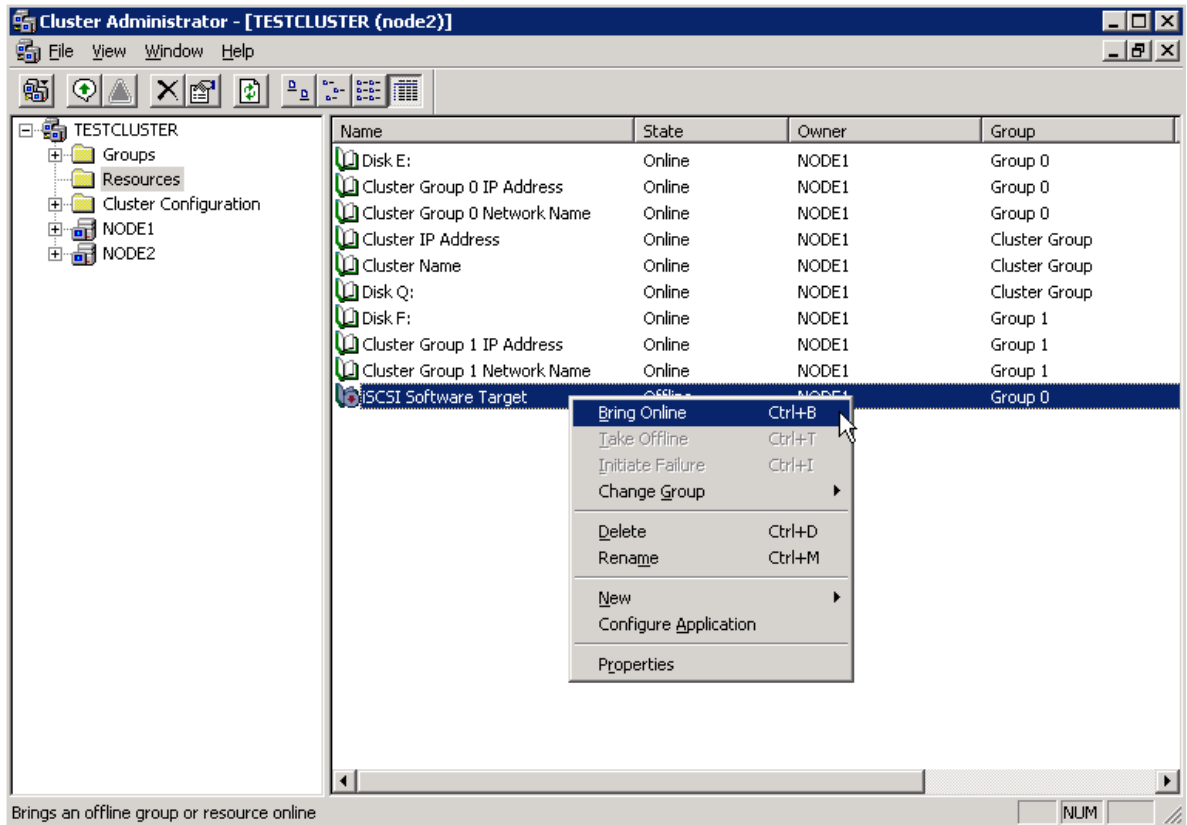
1. Ensure that both cluster nodes are running and that Node 1 is the active node.
2. Log in to Node 1 using an account with administrator privileges.
3. Launch Cluster Administrator (**Start > Programs > Administrative Tools > Cluster Administrator**).
4. Select **Resources**. Right-click and select **New > Resource**.



5. Specify a name and description for this resource on the New Resource page of the wizard.
6. For Resource type, select **Generic Service** from the list.
7. For Group, select the group that contains the resources that are associated with the iSCSI Target(s) that will be created, such as network name, IP address, and physical disk. Click **Next**.
8. On the Possible Owners page, specify Node 1 and Node 2 as possible owners. Click **Next**.
9. On the Dependencies page, select the **Network Name**, **IP Address**, and **Physical Disk (E:\)**. Click **Add**, and then click **Next**.



10. Enter **WinTarget** in the Service name field of the Generic Service Parameters page. Leave the Start parameters field empty. Click **Next**.
11. Click **Add** on the Registry Replication page. Enter **SOFTWARE\Microsoft\iSCSI Target**, and click **OK**.
12. Click **Finish** to make iSCSI Software Target a cluster resource.
13. At this point, the iSCSI Software Target cluster resource should appear as Offline. Right-click the **iSCSI Software Target resource**, and select **Bring Online**.



## Confirm resources failover

1. After the iSCSI Software Target resource comes online, expand the Groups list in the left pane. Right-click **Group 0** and select **Move Group**. Ensure that all Group 0 resources are successfully moved over to Node 2.
2. Repeat the Move Group operation for Group 1 and the Cluster Group. Verify that all Group 0, Group 1, and Cluster Group resources have successfully moved over to Node 2 and that Node 2 is now the active node with full control of all cluster resources.
3. Move Group 0, Group 1, and the Cluster Group back to Node 1. Verify that Node 1 is now the active node with full control of all cluster resources.

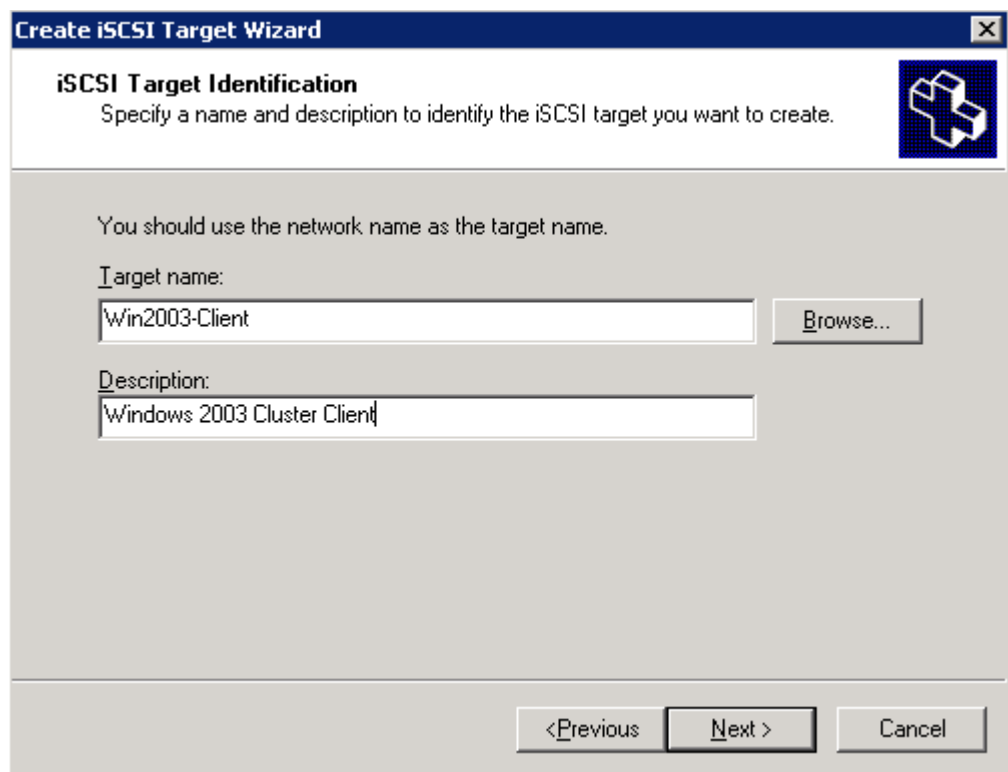
### Note

Microsoft recommends shutting down all nodes in the cluster one at a time and bringing them back online in order to confirm the successful failover of cluster resources. Moving the resource groups allows you to test the failover of resources without completely taking cluster nodes offline.

# Configuring Microsoft iSCSI Software Target

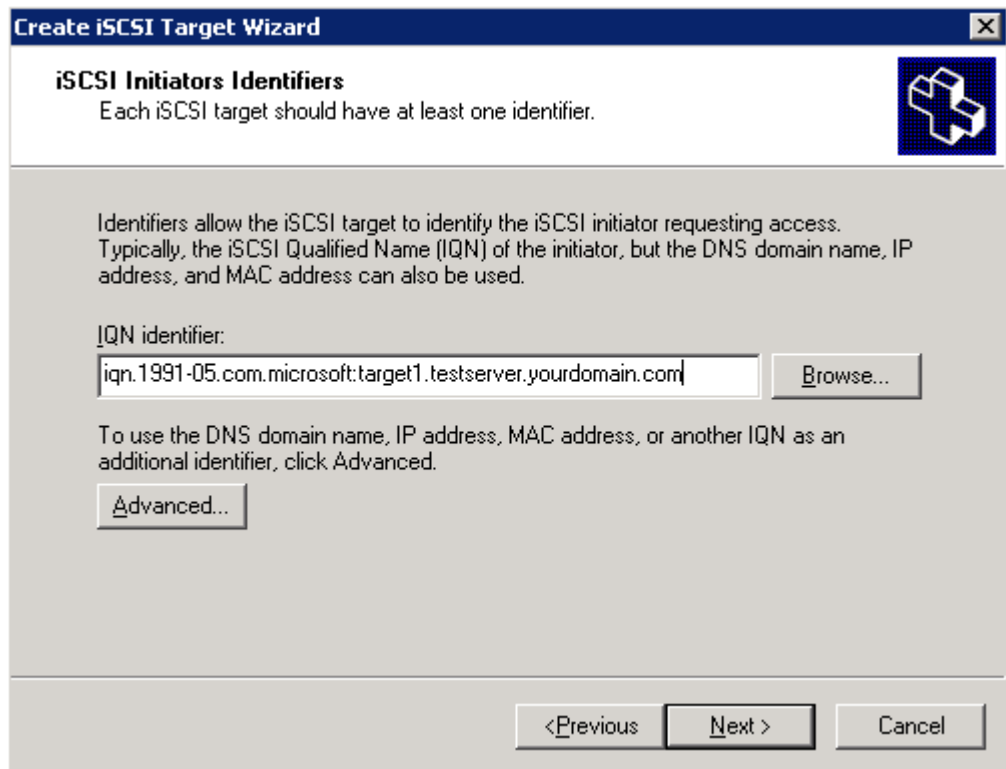
## Creating the iSCSI Target entry

1. Log in to Node 1 with administrative privileges and ensure that it is the active node.
2. Launch the Microsoft iSCSI Software Target Console (**Start > Programs > Administrative Tools > Microsoft iSCSI Software Target**) and select the **iSCSI Targets** node in the left pane.
3. Right-click on the **view page** (right pane), and select **Create iSCSI Target**. Click **Next**.
4. Specify a name for the iSCSI Target that describes the initiator that will be accessing it. You can also enter a description for this host. Click **Next**.



The screenshot shows the 'Create iSCSI Target Wizard' dialog box, specifically the 'iSCSI Target Identification' step. The title bar reads 'Create iSCSI Target Wizard'. The main heading is 'iSCSI Target Identification' with a sub-instruction: 'Specify a name and description to identify the iSCSI target you want to create.' Below this, a note states: 'You should use the network name as the target name.' There are two input fields: 'Target name:' with the text 'Win2003-Client' and a 'Browse...' button to its right; and 'Description:' with the text 'Windows 2003 Cluster Client'. At the bottom, there are three buttons: '<Previous', 'Next >', and 'Cancel'.

5. On the iSCSI Initiators Identifiers page, type the IQN of the initiator machine (found on the General tab of the Microsoft iSCSI Initiator interface). The IQN is used by Microsoft iSCSI Software Target to identify the initiator when it logs in to Microsoft iSCSI Software Target. Click **Next**.



---

**Note**

Click **Advanced** to enter additional identifiers or if you are using an identifier other than an IQN (DNS domain name, IP address, or MAC address).

---

6. Click **Finish** to create the iSCSI Target.

## Exporting an iSCSI virtual disk

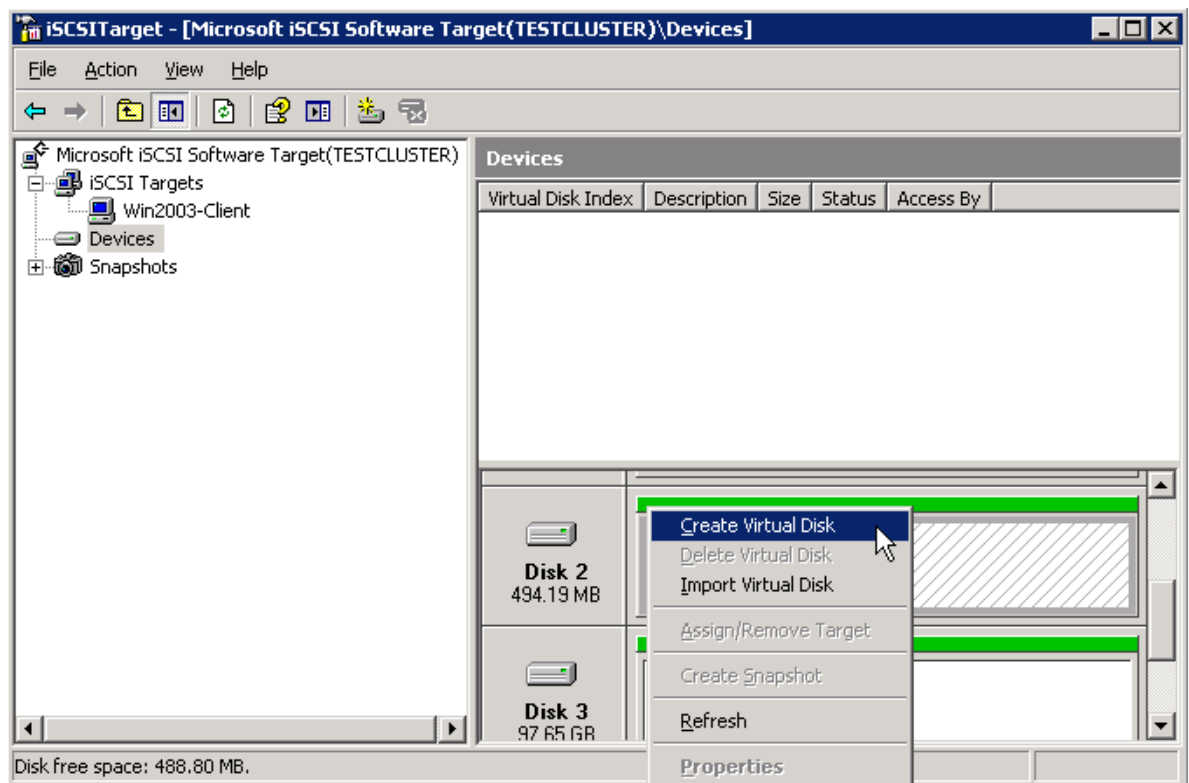
1. Log in to the active cluster node and launch the Microsoft iSCSI Software Target Console.
2. Select **Devices** from the scope item pane.
3. From the Devices view, right-click the empty area of the Devices pane and select **Create Virtual Disk**.

---

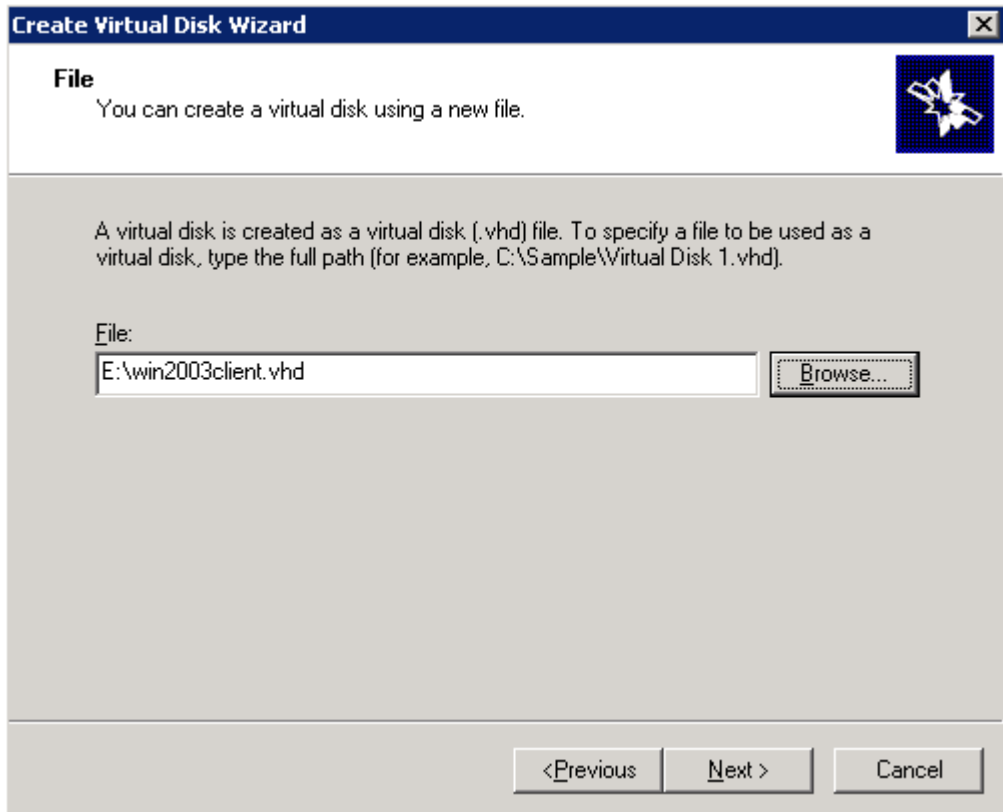
### Note

In order to create iSCSI virtual disks, it is required that physical disks are formatted as NTFS.

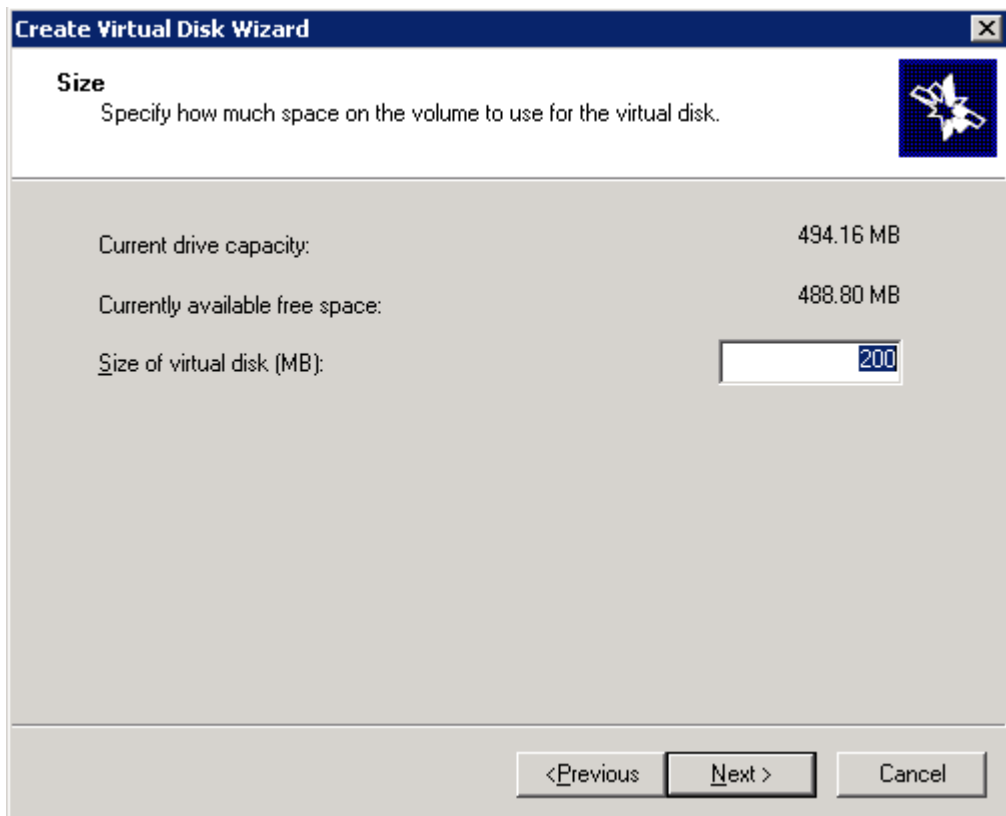
---



4. Click **Next** on the Welcome page.
5. Specify a file name for the virtual disk on the File page of the wizard. Click **Next**.

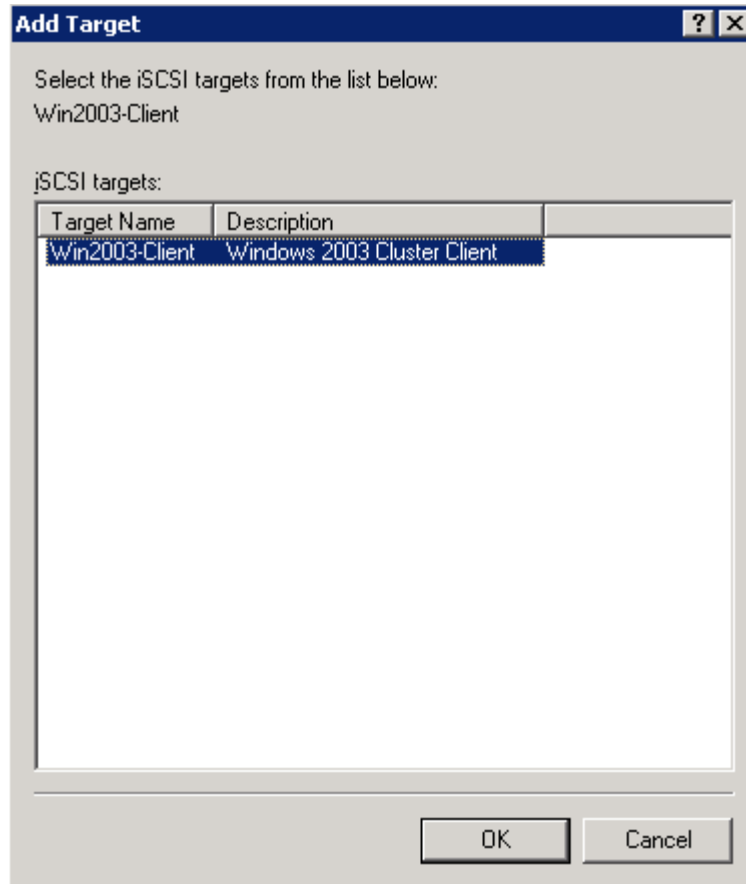


6. On the Size page, enter the size for the Microsoft iSCSI Software Target disk. Click **Next**.



7. Type a description for the virtual disk (optional). Click **Next**.

- Specify the initiator that will have access to the Microsoft iSCSI Software Target disk. Click **Add**, and select the host created in the previous section. Click **OK**, and then click **Next**.



- Click **Finish** to complete the operation.

The newly-created iSCSI virtual disk is ready for use. The final steps involve connecting the initiator to Microsoft iSCSI Software Target.

## Connecting to Microsoft iSCSI Software Target

- On the initiator machine, launch the Microsoft iSCSI Initiator applet.
- Select the Discovery tab. In the Target Portals group, click **Add**. Enter the IP address of the cluster group that is associated with the iSCSI Software Target Resource, and then click **OK**.
- On the Targets page, select the target just added, and click **Log On**. If the target does not appear, click **Refresh**.
- The host is now logged in to Microsoft iSCSI Software Target and the iSCSI device is available for use.

## Configuring advanced features

Microsoft iSCSI Software Target's snapshot feature extends Microsoft Volume Shadow Copy Service (VSS) to enable snapshots (shadow copies) of Microsoft iSCSI Software Target Disks for enhanced data protection. VSS stores shadow copies on an NTFS volume that is user-configurable. To ensure that shadow copies are retained when a failover occurs, the shadow storage area needs to be configured to use a volume on the shared disk device. This section details the steps involved in configuring the shadow storage location.

1. Log in to the active cluster node and launch the Microsoft iSCSI Software Target Console.
2. Select the Devices node. Right-click the first **Microsoft iSCSI Software Target Disk** in the list view, and select **Properties**. The Microsoft iSCSI Software Target Disk properties notebook is displayed.
3. Select the Snapshot Storage tab. This page contains the configuration information for the shadow copies of this Microsoft iSCSI Software Target disk.
4. Ensure that the shadow storage volume is the same as the location of the Microsoft iSCSI Software Target disk file. For example, if the Microsoft iSCSI Software Target disk file path is *E:\win2003client.vhd*, then select **E:\** from the list to be the shadow storage location. Click **OK** to save the settings.
5. Repeat the above steps for other remaining Microsoft iSCSI Software Target disks.

Another advanced feature of Microsoft iSCSI Software Target is the ability to schedule snapshot and local mount operations to occur on a regular basis for backup and restore purposes. Microsoft iSCSI Software Target uses Windows Task Scheduler Service to facilitate this operation. In order for the scheduling configurations to propagate correctly during a failover, the Windows Task Scheduler Service needs to be configured as a cluster resource. This section describes the steps involved.

---

### Important

Configuring Windows Task Scheduler as described in this section will create an active/passive Task Scheduler. This means that Windows Task Scheduler will only run on the active cluster node.

---

The first step is to change the location where Task Scheduler stores the schedule information. By default, this location is the system root folder. This needs to be changed to use the volume on the shared cluster disk.

1. Log in to the active cluster node and launch the Registry Editor.

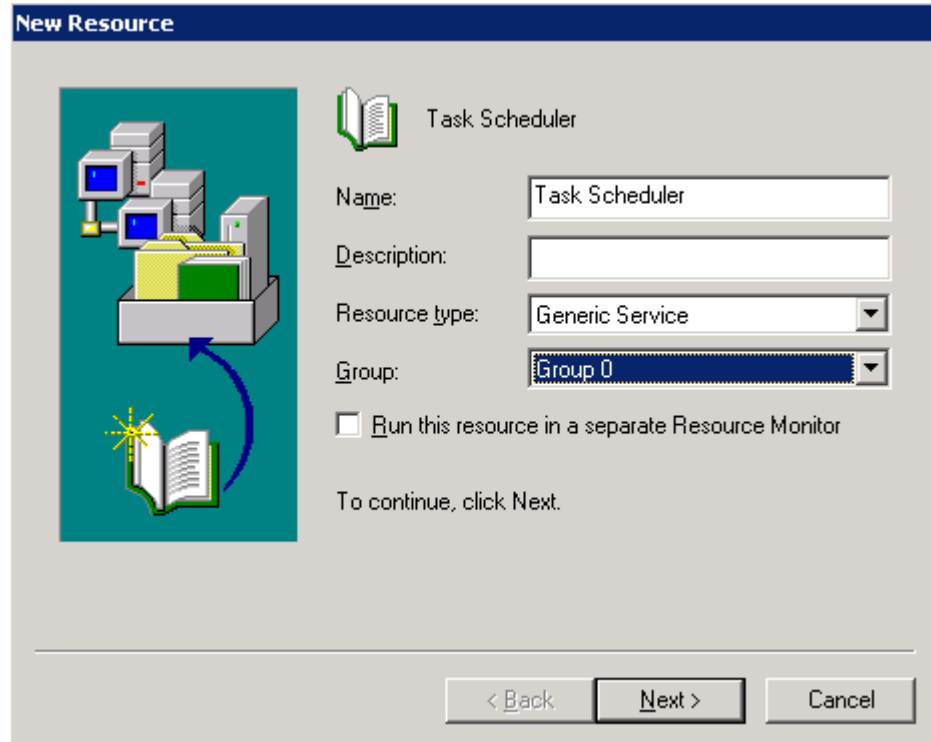
---

### Warning

Improper use of the Registry Editor can render the system unbootable.

---

2. Navigate to **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SchedulingAgent**. Modify the **TaskFolder** value to be the shared disk volume (for example, **E:\Tasks**).
3. Launch Cluster Administrator. Right-click the **Resources** node, and select **New > Resource**.
4. On the New Resource page of the wizard, type a name for the resource (Task Scheduler) and specify the Generic Service resource type. For Group, specify the same group as the volume containing the tasks information (E:\). Click **Next**.



5. For possible owners, specify both cluster nodes. Click **Next**.
6. For dependencies, specify the disk where the task information is stored (**E:\**). Click **Next**.
7. Enter **Schedule** for the service name. Click **Next**.
8. For registry replication, add **Software\Microsoft\SchedulingAgent**. Click **Finish** to create the generic service cluster resource.
9. Right-click the **Task Scheduler** resource, and select **Bring Online**.

---

#### Note

When creating a schedule, ensure that the operation is completed from the active cluster node.

---

---

#### Important

Configuring Windows Task Scheduler as described in this section will create an active/passive Task Scheduler. This means that Windows Task Scheduler will only run on the active cluster node.

---

## For more information

For more information about HP ProLiant Storage Servers, see <http://www.hp.com/go/storageservers>.

© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Itanium is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

4AA1-2898ENW, September 2007

