Configuring a Failover Cluster with Windows Storage Server 2008

Microsoft Corporation

Published: December 2009

Abstract

This document describes how to configure a pair of storage appliances into a failover cluster that will host both a file server and an iSCSI target.

Contents

Configuring a Failover Cluster with Windows Storage Server 2008

Windows Storage Server 2008 provides storage solutions for small, medium, and large organizations. Storage appliances can be configured with a wide variety of hardware, and can be used as individual servers or combined into failover clusters. Windows Storage Server 2008 clusters can host highly available file services, and through the optional Microsoft iSCSI Software Target package, iSCSI block storage.

This paper will guide you through the process of configuring a pair of storage appliances into a failover cluster that will host both a file server and an iSCSI target.

In This Document

Failover Cluster Prerequisites

To create failover clusters using Windows Storage Server 2008, your configuration should meet the following prerequisites:

- Each node should be running the same version of the operating system, including the hardware platform. For example, you might use Windows Storage Server 2008 Enterprise Edition x64 on each node. If you purchase Windows Storage Server 2008 storage appliances for a failover cluster, be sure to purchase matching configurations for each storage appliance.
- Each node should have a minimum of two network adapters, one for cluster heartbeat and the other for supporting the required workload. If you are using iSCSI to provide the shared disks for the failover cluster, you should dedicate another network adapter to the iSCSI traffic.
- Each node should be joined to the same Active Directory domain.

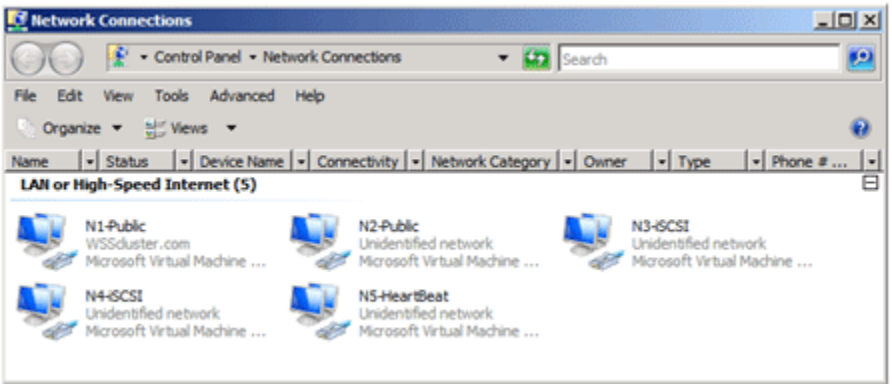
- Each node should have access to a shared storage array using an appropriate interconnect iSCSI, SAS, or Fibre Channel.
- Each node should have access to at least one shared volume to support a witness (quorum) disk that contains a minimum of 500MB of free space and is formatted with NTFS.

As an example in this paper, we will use two storage appliances running Windows Storage Server 2008 Enterprise Edition x64. Each storage appliance will be configured with five network adapters. The example scenario also assumes that you are using iSCSI to connect to shared disks, but does not include configuring the iSCSI target.

Establish a Network Naming Convention

A naming convention will greatly simplify your management of the network connections in your failover cluster. Naming the various network connections to represent the function of each network is particularly useful when many network cards are in use on an individual storage appliance. As a working example, we will use five network ports per cluster node to support client file access and cluster management. We will use the following networks this scenario:

- **N1-Public** attaches to the local area network for client access and remote administration of the cluster. This is the network that clients will use to access the failover cluster.
- **N2-Public** also attaches to the local area network for client access and administration. This secondary port on the same network lets you implement load balancing and redundancy.
- **N3-iSCSI** attaches to an isolated network segment that communicates with the shared iSCSI disks. This network is only for communication between the failover cluster nodes and the iSCSI storage.
- **N4-iSCSI** also attaches to a secondary isolated iSCSI network segment between the cluster nodes and the iSCSI backend. This enables load balancing and redundancy.
- **N5-Heartbeat** attaches to an isolated network segment that is shared among the failover cluster nodes. There should be no other network communication on this network segment. The most typical connection type for the heartbeat segment between the nodes of a two-node failover cluster is a cross-over network cable. If you have more than two nodes in the cluster, you must provide a network hub or switch for the communication.



TCP/IP Network Configuration

The TCP/IP settings for your failover cluster include some that must be configured exactly, and some that permit choices to match your network configuration. The specific recommendations are outlined in the following sections:

Public Network

N1-Public and N2-Public can use either statically assigned TCP/IP settings or the default settings provided through the Dynamic Host Configuration Protocol (DHCP). DHCP is the preferred method of assigning the addresses for the public interfaces, because this will simplify your tasks in configuring the cluster on your network. You should use DHCP-assigned addresses for the physical network adapter's IP address, as well as all virtual IP addresses assigned to virtual servers configured within the failover cluster.

To configure the public network

- No additional network configuration is typically required if DHCP assignment is used, except for setting a reservation in the DHCP scope if you want the cluster to have a consistent address.

Storage Network

N3-iSCSI and N4-iSCSI will typically use static IPv4 addresses, although IPv6 is also fully supported. This scenario will use static IPv4 addresses and disable unnecessary features. In the Properties for N3-iSCSI and N4-iSCSI, make the following changes:

To configure the storage network

1. Set appropriate static IPv4 IP addresses using different private subnet ranges for both N3-iSCSI and N4-iSCSI. For example, you could assign N3-iSCSI a subnet of 192.168.2.0/24 and N4-iSCSI a subnet of 192.168.3.0/24.
2. Deselect unnecessary network features, such as:
   - Client for Microsoft Networks
   - QoS Packet Scheduler
   - File and Printer Sharing for Microsoft Networks
   - Internet Protocol Version 6 (TCP/IPv6), if it is not being used for these connections
3. Disable automatic DNS registration of these connections, because there will be no DNS server on the subnet.

Heartbeat Network

The N5-Heartbeat network is only used for the heartbeat communication between failover cluster nodes. Therefore, you can safely disable most network services for this interface.

To configure the heartbeat network

1. Uncheck the following unnecessary network features:
   - Client for Microsoft Networks
   - QoS Packet Scheduler
   - File and Printer Sharing for Microsoft Networks
   - Internet Protocol Version 4 (TCP/IPv4)
2. Double click Internet Protocol Version 6 (TCP/IPv6).
3. Click the DNS tab.
4. Uncheck **Register this connection's addresses in DNS**, and then click **OK** twice. The IPv6 link local address will be automatically assigned.

Procedures

To modify network connection properties

1. Open **Network Connections**. Click **Start**, right-click **Network**, and then click **Properties**. In **Network and Sharing Center**, click **Change adapter settings**.
2. Open **Properties for a network connection**. Right-click the network connection and then click **Properties**.
3. Highlight the network component to modify and then click **Properties**. To remove a network component, remove the check mark beside the component.
4. Click **OK** to save your modifications.

To disable automatic DNS registration

1. In the **Properties** for N3-iSCSI, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
2. Click **Advanced**, and then click the **DNS** tab.
3. Uncheck **Register the connection's addresses in DNS**, and then click **OK** twice.
4. Repeat these procedures on both N3-iSCSI and N4-iSCSI for all storage appliances that will form the failover cluster.

Prepare the Failover Cluster

This section describes the tasks you need to perform to get ready for creating a failover cluster.

In This Section

Create a Domain User Account

When you first create a cluster or add servers to it, you must be logged on to the domain with an account that has administrator rights and permissions on all servers in that cluster. The account does not need to be a Domain Admins account; it can be a Domain Users account that is in the Administrators group on each clustered server. In addition, if the account is not a Domain Admins account, the account (or the group that the account is a member of) must be given the **Create Computer Objects** permission in the domain.

Note

There is a change in the way the Cluster service runs in Windows Server 2008, as compared to Windows Server 2003. In Windows Server 2008, there is no Cluster service account. Instead, the Cluster service automatically runs in a special context that provides the specific permissions and privileges that are necessary for the service (similar to the local system context, but with reduced privileges). For more information, see http://support.microsoft.com/kb/947049.

Add Nodes to an Active Directory Domain

This is a relatively simple step, but it is required to form any failover cluster. All storage appliances that will become nodes in the cluster must be joined to the same Active Directory domain before you validate the configuration of the failover cluster.

To join an Active Directory domain in Windows Storage Server 2008

1. Open **Computer Properties**. Click **Start**, right-click **Computer**, and then click **Properties**.
2. Under **Computer name, domain, and workgroup settings** click **Change settings**.
3. On the **Computer Name** tab, click **Change**.
4. Under **Member of** click **Domain** and then type the name of the domain to join. Use either the NetBIOS or fully-qualified domain name. For example, to join a domain named Company.local you could type either Company or Company.local.
5. Click **OK**. If the operation succeeds, you will be prompted to restart the computer.

After the storage appliances have joined the domain, you will log on using the domain account you created earlier.

Expose Storage to Cluster Nodes

Each node should have access to at least one disk to support a witness (or quorum) disk and the storage of highly available data. Depending on your backend storage device, you may need to use the storage appliance manufacturer's LUN provisioning tool to provision LUNs and expose them as disks to all nodes in the cluster. The shared disks used for cluster storage must meet the following requirements:

- All shared disks must be on a storage system that is accessible to each node. You can use iSCSI, SAS, or Fibre Channel to make the connection.
- All shared disks must be formatted with one or more NTFS volumes. The witness disk must have an NTFS volume of at least 50 MB, but it is recommended that you allocate 500 MB or more.

If your manufacturer's LUN provisioning tool does not bring disks online or partition and format them, you can use the following procedure to prepare the disks for clustering:

To prepare storage disks for use

1. On one of the storage appliances, open **Disk Management**.
2. Bring the 500-MB witness disk online. Right click the label for the disk and then click **Online**.
3. Initialize the witness disk, selecting either master boot record (MBR) or GUID partition

table (GPT) volume type. Right-click the label for the disk, and then click **Initialize disk**.

4. Create a New Simple Volume. Right-click the disk and then click **New Simple Volume**.
5. Allocate all available capacity for the **Volume Size**.
6. Assign a drive letter to the volume, such as Q:\. The drive letters will not necessarily be the same on every node of the cluster.
7. Click **Perform a quick format**.
8. Click **Finish**.
9. Verify that each storage appliance that will form the failover cluster recognizes the witness disk by viewing the disks in **Disk Management**.

Install the Failover Cluster Feature

Some storage appliances will have the Failover Clustering feature installed by default. If your storage appliances do not have it installed, you must add the Failover Clustering feature before you can continue.

To install the feature, or confirm that it is installed

1. Open **Server Manager**. Click **Start**, click **Administrative Tools**, and then click **Server Manager**.
2. Click the **Features Node** in the left navigation pane.
3. Click **Add Features**.
4. Click the **Failover Clustering** checkbox. If **Failover Clustering** is already checked, it is installed and you can move directly to the next section to begin creating the cluster.
5. Click **Next**.
6. Click **Install**.
7. Repeat these steps on each storage appliance that will form the cluster.

Run Cluster Validation

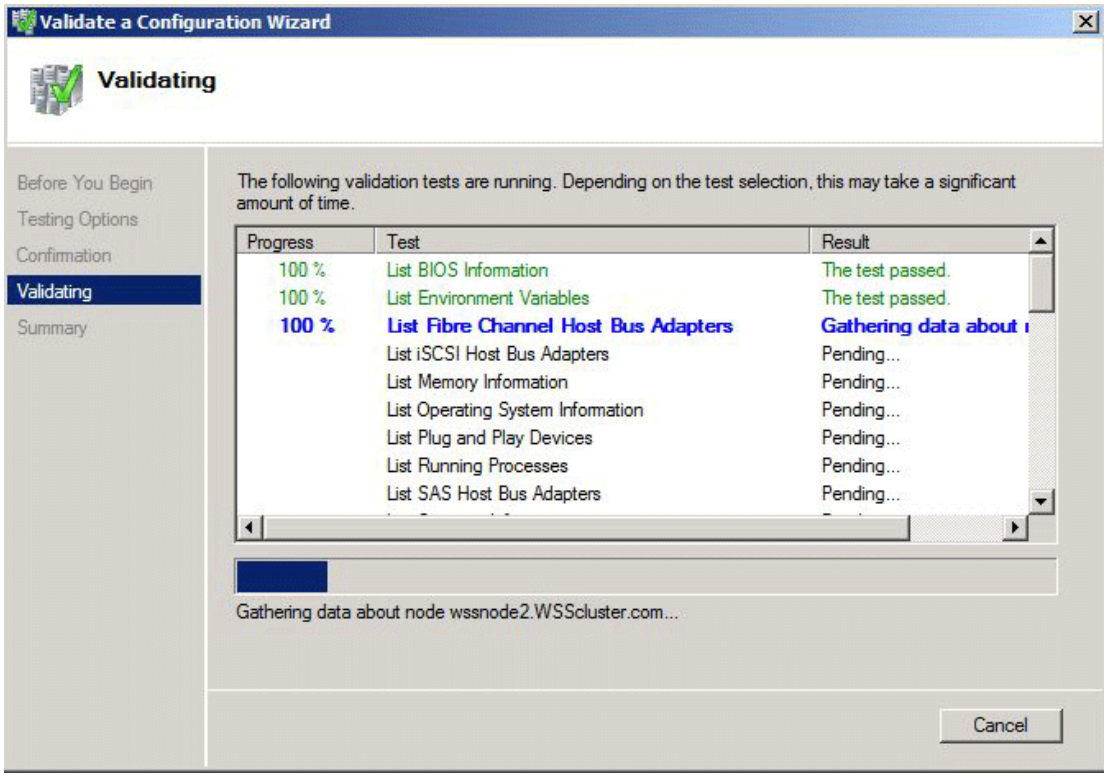
In all cases, you should run the Validate a Configuration Wizard on the storage appliances before forming the cluster. Validation verifies that network, storage, and system configuration requirements are met and that the nodes can form an effective cluster.

Note

If you ever require technical support from Microsoft for failover clustering, you will be asked for the validation report for your failover cluster.

To validate your failover cluster configuration

1. Open the Failover Cluster Management MMC. Click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**.
2. Click **Validate a Configuration**.
3. Click **Next**.
4. In **Enter name**, type a storage appliance name and then click **Add**. Repeat this step for each storage appliance that will form the cluster.
5. Click **Next**.
6. Click **Next** to run all tests.
7. Click **Next** to confirm test requirements. If there are any errors or warnings, you should review the validation report and resolve the issues before creating the cluster. Be sure to run the Validate a Configuration Wizard again to verify that all issues have been resolved.



Create and Configure the Failover Cluster

This section describes how to create a failover cluster and configure services for the cluster to provide to clients. Before you begin these steps, make sure that you have completed all the preparatory steps described in Prepare the Failover Cluster, including running the Cluster Validation Wizard. If you ever require technical support from Microsoft for failover clustering, you will be asked for the validation report for your failover cluster.

In This Section

Create a Cluster

Assuming your selected failover cluster configuration has passed the validation tests, creating the cluster is simply a matter of completing the wizard.

To create a failover cluster

1. Open the Failover Cluster Management MMC. Click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**.
2. Click **Create a cluster**.
3. Click **Next**.
4. In **Selected server**, type the name of each storage appliance that will become part of the cluster.
5. After all nodes are listed, click **Next**.
6. Type a cluster name and deselect all networks, and then click **Next**.
7. Click **Next** to confirm the operation.
8. Click **Finish** to close the summary. You can also choose to view the report to see all of the operations that were performed.

Set Cluster Network Properties and Apply Naming Convention

After you have created the failover cluster, you should configure the network usage in Failover Cluster Management. This step tells the cluster which network connections are used by the cluster, and which are available for network access by clients.

To configure your network connections in Failover Cluster Management

1. Open Failover Cluster Management. Click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**.
2. Expand the **Networks** node.
3. Right click a network and then click **Properties**.
4. Under **Name**, type the corresponding network name for the connection. This should match the network connection naming convention you created earlier.
5. Click the appropriate network options for the connection. You can refer to the table below for the information used in this scenario.

Note

By default, only networks configured with a default gateway will be set automatically to **Allow Clients to connect through this network**. The network connections you create for your public network (that is, the connections clients use to connect to the cluster) will have a default gateway address whether you statically assign the addresses or use DHCP. The isolated network segments used for iSCSI and heartbeat communication do not have default gateways assigned. When you create your failover cluster, the wizard should correctly configure these networks based on the addressing used.

This scenario uses the following settings:

Network	Function	IP address	Allow cluster to use this network	Allow clients to connect through this network
N1-Public	File	192.168.1.#/24	Yes	Yes
N2-Public	File	Optional subnetTeaming	Yes	Yes
N3-iSCSI	iSCSI	192.168.2.#/24	Yes	No
N4-iSCSI	iSCSI	192.168.3.#/24	Yes	No
N5-Heartbeat	Heartbeat	Fe80::8841:71c6…192.168.4.#/24	Yes	No

Create a Highly Available File Server

The purpose of a high availability file server is to ensure that files stored within it are always available to clients, even in the event of hardware failure on the server. When you use a failover cluster to host a file server, the file server becomes a service that can be immediately transferred to another cluster node if the owner node suffers a failure or otherwise becomes unavailable. In this section, we will use one of the additional shared disks you created earlier to provide file server storage in the cluster and configure the file server application within the failover cluster.

Steps for Creating a Highly Available File Server

You should already have the File Services role installed on the nodes of your failover cluster. If you do not, or if you need to verify that the role is installed, use the following steps.

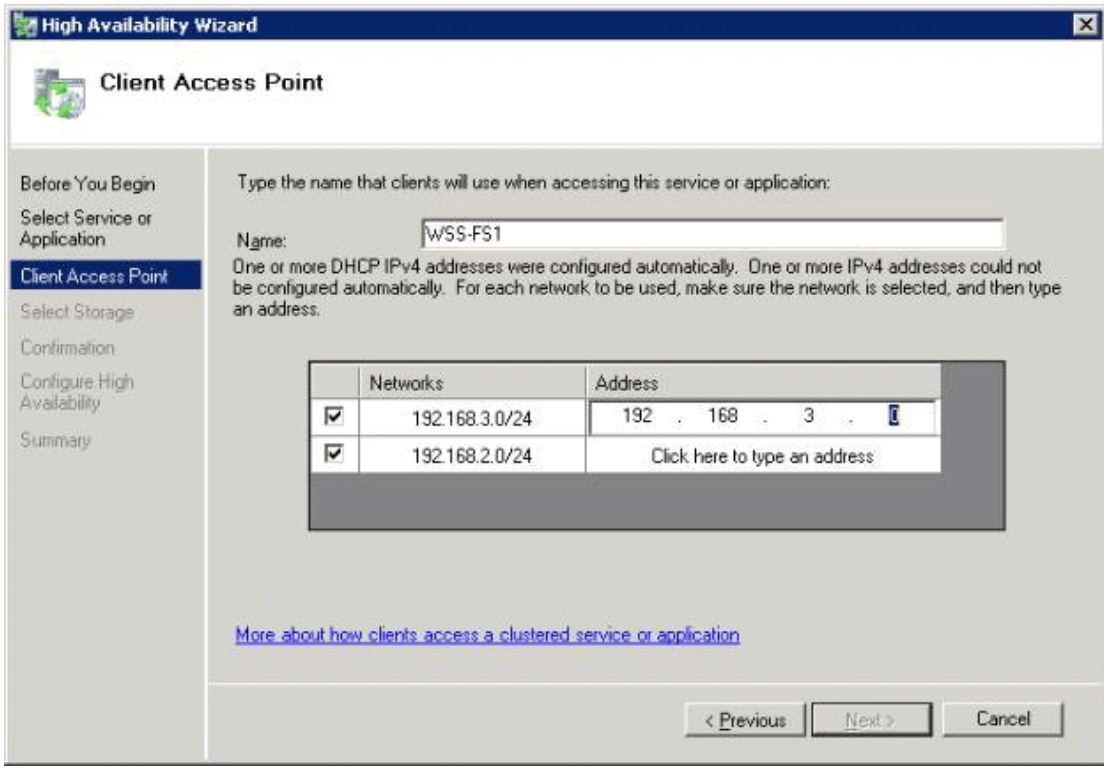
To install the File Services role

1. Open **Server Manager**. Click **Start**, click **Administrative Tools**, and then click **Server Manager**.
2. Click the **Roles** node, and then click **Add Roles**. Click **Next**.
3. Click the **File Services** checkbox, if it is not already selected, and then click **Next**.
4. Click all the appropriate **Role Services** for your cluster to provide (such DFS, FSRM, NFS, and so on), and then click **Next**.
5. Click **Install**.
6. When the wizard completes, click **Close**. Repeat these steps on each node of the cluster.

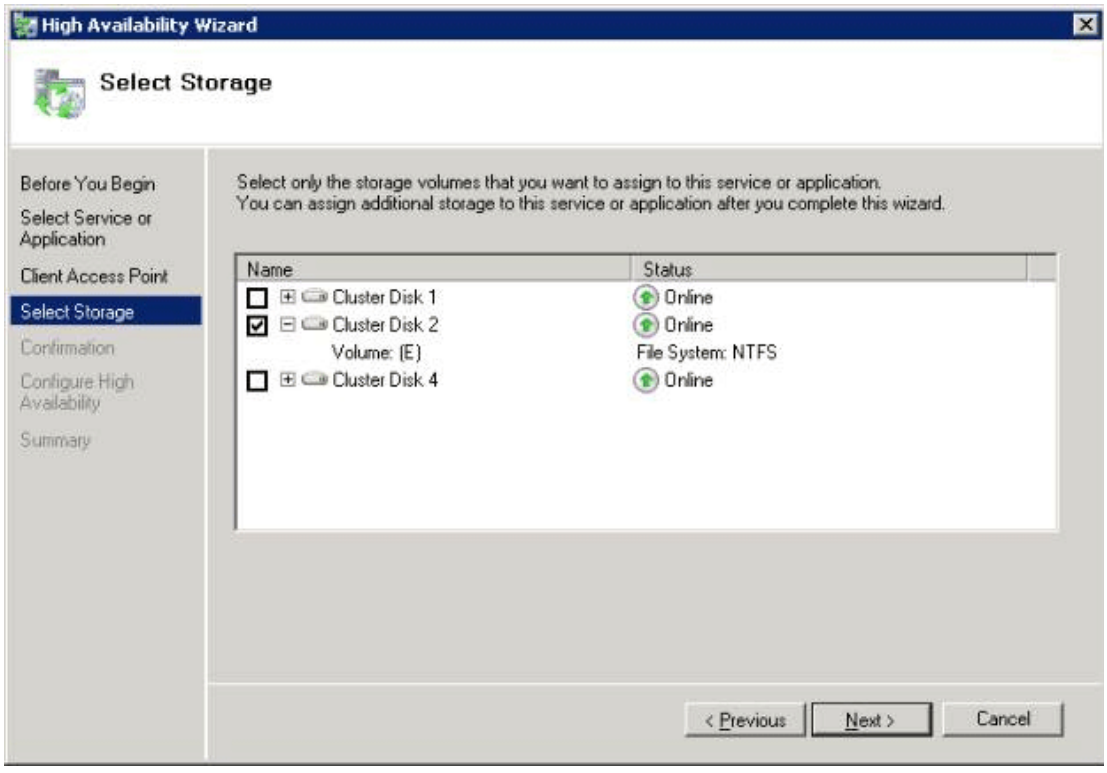
Creating a high availability file server is relatively straightforward in a cluster configuration. You need to configure one or more disks, an IP address (typically assigned via DHCP), and a network name that users will connect to.

To create a highly available file server

1. Open Failover Cluster Management. Click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**.
2. Click the **Services and Applications** node, and then click **Configure a Service or Application**.
3. Click **Next**.
4. Click **File Server** from the available list and then click **Next**.
5. In **Name**, type a file server name (WSS-FS1 in this example). If you are prompted to specify the networks to use, you should uncheck all statically assigned networks, because they represent isolated networks that clients cannot access. Click **Next**.



6. Select one of the available disks to allocate to the file server, and then click **Next**.



7. Click **Next** to confirm the operation.
8. Click **Finish**.

To create a share on the cluster for SMB/CIFS client access

1. Open Failover Cluster Management. Click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**.
2. Expand the **Services and Applications** node to show the highly available file server you created earlier.
3. Highlight the file server to display resources.
4. In the **Actions** pane, click **Manage shares and storage**.
5. In **Share and Storage Management**, click **Provision Share**.
6. Follow the instructions in the wizard. These instructions will depend on the files services you selected when installing the File Services role.

Mapping User Folders to the Highly Available File Server Share

Users can now access the highly available file server by manually mapping to the SMB share created in the previous step, or automatically via a logon script. The users should be directed to \\<*highly available file server name*>\Users\%username%, where <*highly available file server name*> corresponds to the name you applied to your file server in Failover Cluster Management. For information about creating a logon script, see Creating logon scripts

Connecting to the file server you created in Failover Cluster Management (instead of connecting to the cluster name or to any of the nodes in the cluster) may not be intuitive for your users. The purpose of the highly available file server is to be online regardless of the specific server hosting the service, and so the connection is made to the service rather than to a physical computer.

Create a Highly Available iSCSI Target

Your Windows Storage Server 2008 storage appliance can serve as an iSCSI target if it has Microsoft iSCSI Software Target 3.2 installed. Microsoft iSCSI Software Target can be used with a failover cluster to provide a highly available iSCSI target for other servers to use.

Your storage appliance may already have Microsoft iSCSI Software Target installed, depending on the configuration provided by the manufacturer. Microsoft iSCSI Software Target is a separately available package for Windows Storage Server 2008. If it is not provided as part of the storage appliance configuration you purchased, it can be acquired from the manufacturer of your storage appliance.

To create the highly available iSCSI target, you must meet the following prerequisites:

- The Firewall ports must be set on the Storage Server 2008 systems to allow iSCSI initiators to communicate with the Microsoft iSCSI Software Target.
- Version 3.2 of the Microsoft iSCSI Software Target must be installed on all Windows Storage Server 2008 systems that are intended to form the failover cluster. Before you install Microsoft iSCSI Software Target, the Windows Firewall must be configured as described below.
- There must be at least one clustered disk listed in **Available Storage** under the **Storage** node in the Failover Cluster Management MMC.

Configuring Windows Firewall for Microsoft iSCSI Software Target

Before you install the Microsoft iSCSI Software Target, you must configure the Windows Firewall to allow the necessary network traffic to pass. The following table lists the required ports:

Port or application	Description
TCP 3260	Microsoft iSCSI Software Target Service. This port provides the primary access to the Microsoft iSCSI Software target.
TCP 135	Remote Procedure Call (RPC). This port is required for Component Object Model (COM) communication.
UDP 138	NetBIOS Datagram Service. This exception should already exist for the File and Print Service role, but may need to be added manually if not present.
%windir%\System32\Wintarget.exe	Microsoft iSCSI Software Target Service.
%windir%\System32\WTStatusProxy.exe	Microsoft iSCSI Software Target status proxy.

Note

You may get RPC errors when trying to remotely manage a Microsoft iSCSI Software Target if you do not configure the Windows Firewall exception for WTStatusProxy.exe.

The following table contains the Windows Firewall exception that should be made on the iSCSI initiator computer.

Application exception	Description
%windir%\System32\Wtvds.exe	The Microsoft iSCSI Software Target VDS Hardware Provider.

To add an inbound filter rule for a program

1. Open Windows Firewall with Advanced Security. In **Server Manager**, expand **Configuration**, expand **Windows Firewall with Advanced Security**, and then click **Inbound Rules**.
2. In the **Actions** pane, click **New Rule**.
3. Under **What type of rule would you like to create**, click **Program**, and then click **Next**.
4. Click **Browse**, browse to the %windir%\System32 folder, and then click **Wintarget.exe**. Click **Open** and then click **Next**.
5. Click **Allow the connection**, and then click **Next**.
6. Select the network locations that should be bound to this rule (the default is **Domain**, **Private**, and **Public**). Click **Next**.
7. Under **Name**, type a descriptive name for the rule. For example, type Microsoft iSCSI Software Target Service for the program rule for Wintarget.exe. Click **Finish**.

To add an inbound filter rule for a port

1. Open Windows Firewall with Advanced Security. In **Server Manager**, expand **Configuration**, expand **Windows Firewall with Advanced Security**, and then click **Inbound Rules**.
2. In the **Actions** pane, click **New Rule**.
3. Under **What type of rule would you like to create**, click **Port**, and then click **Next**.
4. Select the protocol for this rule, either TCP or UDP. Under **Does this rule apply to all local ports or specific local ports**, click **Specific local ports** and type in the appropriate port number.
5. Click **Allow the connection**, and then click **Next**.
6. Select the network locations that should be bound to this rule (the default is **Domain**, **Private**, and **Public**). Click **Next**.
7. Under **Name**, type a descriptive name for the rule. For example, type Remote Procedure Call for the RPC communication on TCP port 135. Click **Finish**.

Installing the Microsoft iSCSI Software Target

The Microsoft iSCSI Software Target version 3.2 is available as an optional package for Windows Storage Server 2008. You can obtain the Microsoft iSCSI Software Target package from the original equipment manufacturer (OEM) of your storage appliance.

To install Microsoft iSCSI Software Target on your storage appliance, double-click the iscsitarget.msi file and follow the prompts.

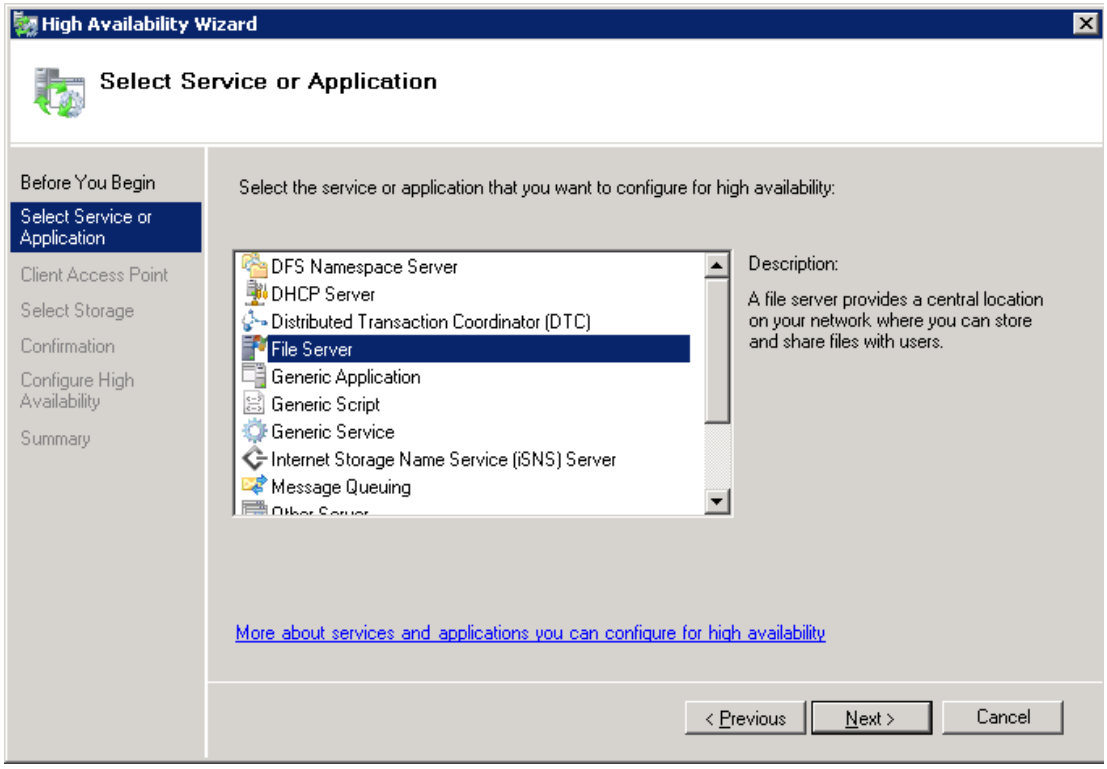
For more information about Microsoft iSCSI Software Target, see the Microsoft iSCSI Software Target Getting Started Guide (http://go.microsoft.com/fwlink/?LinkId=169726).

Create the Failover iSCSI Target Resource Group

To make Microsoft iSCSI Software Target available on your failover cluster, the service must be defined in Failover Cluster Management. The storage that will form the iSCSI volumes must be on the share storage and visible to each node in the cluster. Install the same version of the Microsoft iSCSI Software Target on each node before continuing.

To create an iSCSI resource group

1. In Failover Cluster Management, select the **Services and Applications** node. In the **Actions** pane, click **Configure a Service or Application** to launch the High Availability Wizard.
2. On the **Before You Begin** page, click **Next**.
3. Click **Other Server** and then click **Next**.



4. Enter a name for the iSCSI resource group (WSS-iSCSI1 for this scenario) and then click the IP addresses that will be used for the target to support iSCSI initiator connectivity. Click **Next**.

Note

The IP addresses displayed in the Client Access Point are for networks that

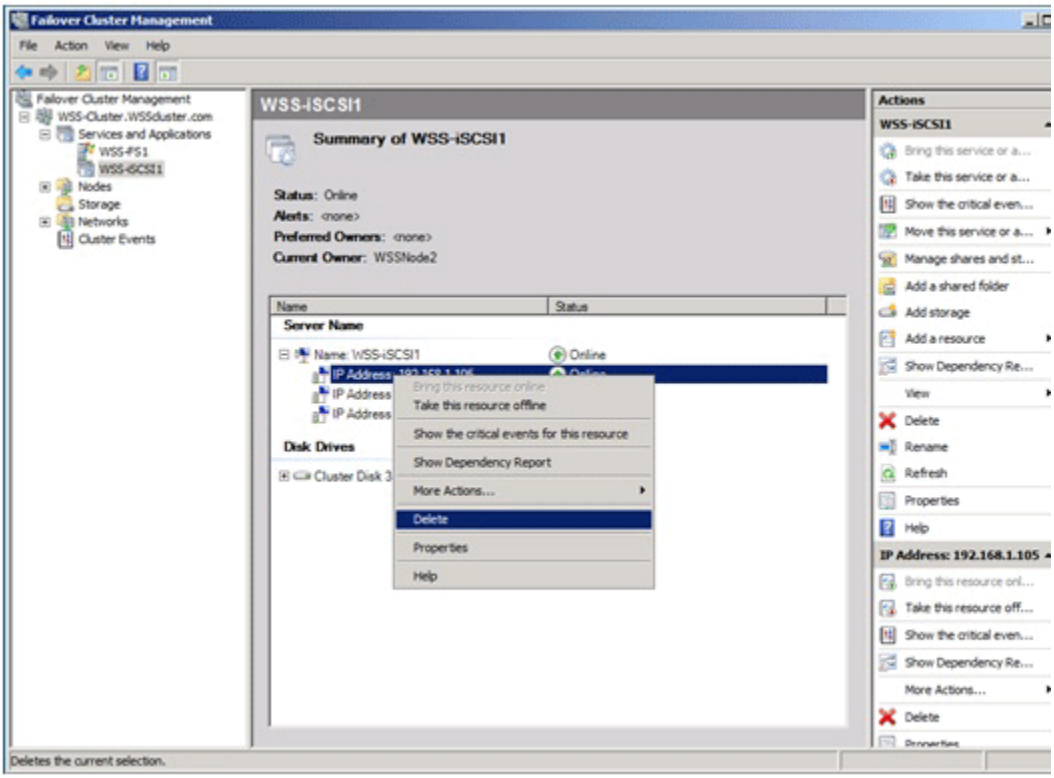
do not have a DHCP address assignment. Only statically assigned networks will be displayed here and can be selected or deselected as required to support a high availability iSCSI infrastructure. In the example above both 192.168.2.20 and 192.168.3.20 will be registered to the highly available iSCSI resource group. These will be the IP addresses that initiators will use to establish connectivity. This example is using the same iSCSI networks that the cluster uses to communicate with the iSCSI backend storage. You should consider dedicating a separate network segment to provide iSCSI network communication between the target and the initiators to provide the best performance.

5. Select one or more storage devices to be used to support the highly available iSCSI resource group. Click **Next**.

   Note

   The clustered disk(s) listed in the above window are from the available storage pool as listed under the **Storage** node within the Failover Cluster Management MMC. If no disks are listed check that there is Available Storage within the Cluster Management MMC, if nothing is listed provision a shared disk to support the highly available iSCSI resource group.

6. Do not click either option on the **Select Resource Types** page; they will be added automatically. Click **Next**.
7. Click **Next** to confirm the selection.
8. Optionally select **View Report** for summary details, or click **Finish** to close the High Availability Wizard.
9. In Failover Cluster Management, under the **Services and Applications** node, expand the iSCSI highly available resource group to display its resources. Delete the DHCP-assigned IP address if it is not required to support iSCSI target access, such as when the iSCSI network communication will be limited to isolated statically addressed network segments.



Create an iSCSI Target in the Microsoft iSCSI Target MMC

Microsoft iSCSI Software Target 3.2 lets your Windows Storage Server 2008-based failover cluster become a high availability iSCSI storage device. After you have created the resource group to automatically fail over the Microsoft iSCSI Software Target between nodes of the cluster, you must define iSCSI targets that clients will connect to.

Note

Ensure that the iSCSI resource group is owned by the node where you launch Failover Cluster Management. Otherwise, configuration will not be available.

To create an iSCSI target in the MMC

1. Open Microsoft iSCSI Software Target on one of the Windows Storage Server 2008 failover cluster nodes. Click **Start**, click **Administrative Tools**, and then click **Microsoft iSCSI Software Target**.
2. In the **Navigation** pane, highlight the **iSCSI Targets** node. Click **Create iSCSI Target**,

then click **Next**.

3. Type a descriptive iSCSI target name and select **Next**.

   Note

   The iSCSI target name should not be the same as the name you used to create the iSCSI resource group in the failover cluster MMC.

4. Click **Browse** to list available Initiators. If no initiators are configured yet, you can type a single character to use temporarily. If you know the name that will be used for the initiator, you can use it here. You can use the IP address, DNS name, or MAC address to specify the initiator by clicking **Advanced**. Click **Next**.
5. Under **Resource group**, select the appropriate resource group. This is the group name you provided when you created the iSCSI target resource group in Failover Cluster Management. Click **Next**.
6. Click **Finish** to complete the configuration of the Microsoft iSCSI Software Target.
7. Expand the **iSCSI Targets** node in the Microsoft iSCSI Software Target MMC to display the target.

Create and Configure Virtual Disks

Once Microsoft iSCSI Software Target is running and configured on your failover cluster, you will want to connect an iSCSI initiator to the targets. If you are connecting to the Microsoft iSCSI Software Target from a Windows operating system, use the following steps. For other operating systems, consult the instructions provided with your iSCSI initiator.

To create a virtual disk for the iSCSI target

1. In Microsoft iSCSI Software Target, select the iSCSI Target you previously created. Click **Create Virtual Disk for iSCSI Target**. Click **Next**.
2. Type a valid path to the disk used to support the iSCSI resource group and then click **Next**.
3. Type a size for the virtual disk in megabytes (MB), and then click **Next**.
4. Type a description for the virtual disk and then click **Next**.
5. Click **Add**, select the relevant iSCSI target created previously, click **OK** to confirm selection, and then click **Next**.
6. Select **Finish** to close the Create Virtual Disk Wizard.

Connect Initiators

After Microsoft iSCSI Software Target is running and configured on your failover cluster, you will want to connect an iSCSI initiator to the targets. If you are connecting to the Microsoft iSCSI Software Target from a Windows operating system, use the following steps. For other operating systems, consult the instructions provided with your iSCSI initiator.

To connect an iSCSI initiator to the targets in Microsoft Windows

1. On the computer you want to connect to the iSCSI target, open the iSCSI initiator. Click **Start**, click **Administrative Tools**, and then click **iSCSI Initiator**.
2. Click the **Discovery** tab.
3. Select **Add Portal**, enter one of the IP addresses for the target as assigned in the Client Access Point Cluster High Availability Wizard (either 192.168.2.20 or 192.168.3.20 for this scenario).
4. Click the **Targets** tab.
5. Highlight the target created previously, which should have an **Inactive** status, and then click **Log on**.
6. Click **Automatically restore this connection when the computer starts** and then click **OK**.
7. Click **OK** to close the iSCSI initiator.

Your initiator should now have access to the volumes provided by the iSCSI target. To verify this, and to prepare the disks for use, use the following steps.

1. In Server Manager, expand the **Storage** node and then click **Disk Management**. You should see a new disk in an **Offline** state.
2. Bring the disk online by right clicking its label and then clicking **Online disk**.
3. Initialize the disk by right clicking its label and then clicking **Initialize disk**. Choose the appropriate partition type (MBR or GPT), depending on the size of the volume. GPT should be chosen if the volume size will be larger than two terabytes (TB).
4. Create a new simple volume by right clicking the drive and then clicking **New Simple Volume**. Allocate all available capacity for the volume size. Click **Next**.
5. Assign a drive letter to the volume. Click **Next**.
6. Click **Perform a quick format**. Click **Next**.
7. Click **Finish**.

Microsoft iSCSI Software Target Performance Recommendations

To get the best performance from your highly available Microsoft iSCSI Software Target installation, use the following tips:

- Distribute resource groups evenly across cluster nodes. This assumes that you have more than one resource group created for multiple targets. Divide the resource groups across nodes so that the workload is not performed by a single storage appliance.
- Use IPSec sparingly. IPSec can provide a high level of security for iSCSI communication, but it does add a small hit to performance. Only implement IPSec on iSCSI connections where security is a concern.
- Enable multipath input and output (MPIO) to provide performance and higher availability. By using two or more ports for the iSCSI network communication, such as the two subnets we used in this scenario, you can enable MPIO to ensure that the iSCSI volume is available even if a single network connection fails.
- Use static IP addresses for iSCSI network connections. You can use DHCP for the iSCSI addresses, but you should also create address reservations for the ports so that they have a consistent address.
- Only assign one initiator to a target, except in cases where the target will support shared storage for a cluster.

Testing Your Failover Cluster Configuration

Now that you've created a failover cluster and configured high availability applications, you can test your cluster's failover ability in Failover Cluster Management. Use the following steps to test failover.

To move a service to another node

1. Open Failover Cluster Management. Click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**.
2. Expand the **Services and Applications** node and click the service or application to test.
3. In the **Actions** pane, click **Move this service or application to another node** and then click the node to move to.

If the move operation completes successfully, there will be no errors or warnings and the summary view of the service or application will update the **Current Owner** field to show the new node's name.