Seagate Business Storage Windows Server 4-Bay NAS

Administration Guide

Seagate Business Storage Windows Server 4-Bay NAS Administration Guide

Regulatory Compliance

FCC Class B Information

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: **FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

IMPORTANT NOTE: (For mobile device use)

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE IMPORTANTE: (Pour l'utilisation de dispositifs mobiles)

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Battery Safety

This product contains a lithium-ion battery that must be disposed of properly.

Please follow the battery safety items below:

- Do not dismantle, open or shred secondary cells or batteries.

- Do not expose cells or batteries to heat or fire. Avoid storage in direct sunlight.

- Do not short-circuit a cell or a battery. Do not store cells or batteries haphazardly in a box or drawer where they may short-circuit each other or be short-circuited by, other metal objects.

- Do not use any charger other than that specifically provided for use with the equipment.

- Do not use any cell or battery which is not designed for use with the equipment.

- Do not mix cells of different manufacture, capacity, size or type within a device.

- Seek medical advice immediately if a cell or a battery has been swallowed.

- Do not subject cells or batteries to mechanical shock.

- In the event of a cell leaking, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with copious amounts of water and seek medical advice.

- Keep cells and batteries out of the reach of children.

- Keep cells and batteries clean and dry.

- Secondary cells and batteries need to be charged before use. Always use the correct charger and refer to the manufacturer's instructions or equipment manual for proper charging instructions.

- Do not leave a battery on prolonged charge when not in use.

- After extended periods of storage, it may be necessary to charge and discharge the cells or batteries several times to obtain maximum performance.

- Secondary cells and batteries give their best performance when they are operated at normal room temperature (20°C+5 °C).

- Retain the original product literature for future reference.

- Use only the cell or battery in the application for which it was intended.

- Dispose of properly.

The Seagate Wireless Plus device is not intended for office use.

Contents

1.   Setup

Congratulations on your purchase of a Seagate® Business Storage Server. Your Seagate server takes full advantage of the rich set of network administration tools offered by Windows Storage Server 2012 Workgroup (WSS 2012). In addition to data sharing and backup, your Seagate server can join active directories, replicate data across LANs and WAN, and configure hard drives using advanced storage pools.

To set up your Seagate server, you must connect directly to the server with a keyboard, display, and mouse. After the initial setup, you can connect to the server using Remote Desktop from a network-connected Windows or Mac computer or a compatible mobile device.

See the Quick Start Guide and the user manual for details about connecting the hardware. For additional questions regarding hardware, go to Seagate Customer support.

Powering On for the First Time

1. On the front of the server, press the **Power** button.

    The first time you power on the server, the front LCD panel displays Initializing the system and then Starting. The monitor displays Settings.

2. Follow the on-screen instructions for Windows Storage Server 2012.

Each time you boot up the server, it displays the Seagate NAS Configuration Tasks window. The window contains links to configuration tools. If you prefer to not access these tools through the Configuration window, select **Do not show this window at the next logon** at the bottom of the window.

Note: Selecting **Do not show this window at the next logon** has a permanent effect. The next time you reboot, the Configuration Tasks window does not appear, and you cannot recover it.

Server Manager Admin Tool

The NAS Server Manager GUI allows you to administer most Windows Storage Server tasks easily.

To access Server Manager tools:

1. Drag the cursor to the left-bottom corner of the screen. Start appears.

2. Do one of the following:

    •   Right-click **Start** and choose the tool you want to access from the list.

- Click **Start** to open tiles view, and type the tool, feature, or file that you want to view.

To access Server Manager, click its icon in the Task bar

Note: You can use the command-line interface Windows PowerShell to perform administrative tasks. How to use PowerShell cmdlets is beyond the scope of this manual.

Connecting Remotely

After the initial configuration, you can connect to your server and perform administration tasks using Microsoft Remote Desktop. You can perform most administration tasks remotely with the Server Manager. However, you cannot repair or reinstall Windows remotely.

You can use Remote Desktop to control your NAS remotely via a computer on your WAN. The instructions vary depending on your network configuration and your network security. If you experience problems, try to use a static IP Address on your remote computer and open port 3389 on the server.

To use Remote Desktop, the following network requirements are recommended:

- DHCP server for automatic remote server setup

- Gigabit Ethernet routers, peripherals, and computer network interfaces

Remote Desktop via Windows

Remote Desktop is available on Windows XP, Windows Vista, Windows 7, and Windows 8. The following are required:

- Pentium or equivalent processor (1GHz or higher)

- 512MB of RAM or more

- Connection to the same network as the NAS

Connect to your Seagate NAS remotely

1. From the Start menu, select **All Programs > Accessories > Remote Desktop Connection**.

   The Remote Desktop Connection dialog box opens.

2. Click **Show Options**.

3. On the General tab, select your NAS from the Computer list.

4. If necessary, enter **Administrator** as the user name.

5. To save these settings for the next connection, click **Save**.

---

6. Click **Connect**.

You might receive a warning message about the identity of the remote computer (your NAS). To prevent this message from appearing again, select **Don't ask me again for connections to this computer** and click **Yes**.

7. Enter your NAS Administrator password and click **OK**.

The Seagate NAS - Remote Desktop Connection window opens.

Remote Desktop via Other Platforms

Microsoft also supports remote connection clients for other platforms:

- iPads and iPhones
- Android devices
- Macintosh desktops and laptops

For details on using other clients, go to the Microsoft support website and search for "Microsoft remote desktop clients."

You also might be able to establish a remote desktop connection using a Windows emulation application on Mac or Linux.

2. Administrators and Users

After the initial setup, your server has only an Administrator account. The Administrator can create other administrators, users, and groups.

Administrators

Administrators have full access to all WSS 2012 functions, settings, and files. An administrator can:

- Change all server settings

- Create and modify user accounts

- Create and modify groups

- Set up and modify folders and shares

- Assign and modify system permissions, including granting users administration capabilities

- Install software

- Update the server's firmware

- Reset the server's name and password

Users

By default, users can:

- Change their login password

- Save and share files on the server

- Back up files to the server

- Access the server over the web

An administrator can grant a user additional privileges.

Create a user

To create a user account, you must be logged in to the server as an administrator.

1. In the upper right of the Server Manager Dashboard, select **Tools > Computer Management**.

2. Under Computer Management, select **System Tools > Local Users and Groups**.

3. Select the **Users** folder.

The center panel displays a list of users.

4. In the Actions panel, under Users, select **More Actions > New User**.

5. In the New User dialog box, enter the information for the new user and click **Create**.

Modify user properties

1. In the Server Manager center panel, select the user account to modify.

2. In the Actions panel, select **[User name] > More Actions > Properties**.

3. In the Properties dialog box, make the changes, and click **OK**.

Groups

An administrator can grant a group of users access rights to resources on the server. Granting an access right to a group gives all members of the group the same access right. Assigning users to groups can simplify configuration tasks.

Create a group

To create a group, you must be logged in to the server as an administrator.

1. In the upper right of the Server Manager Dashboard, select **Tools > Computer Management**.

2. Under Computer Management, select **System Tools > Local Users and Groups**.

3. Select the **Groups** folder.

   The center panel displays a list of users.

4. In the Actions panel, under Groups, select **More Actions > New Group**.

5. In the New User dialog box, type a group name.

   The name cannot contain spaces. You can optionally enter a description.

6. Click **Create**.

7. In the Object Names text box, enter a user name, and then click **Check Names**.

   The name is displayed with its server path.

8. Click **OK**.

9. Repeat for additional users that you want to add to the group.

10. Click **Create**, and then click **Close**.

Modify group properties

1. In the Server Manager center panel, select the group to modify.

2. In the Actions panel, select **[Group name] > More Actions > Properties**.

3. In the Properties dialog box, make the changes and click **OK**.

3. Managing Storage

Your Seagate server has predefined volumes. One volume is used for the Windows system software, and another is for data. You cannot modify the system volume, but you can reconfigure the data volume.

RAID Versus Storage Pools

With WSS 2012, you can group physical hard drives into storage pools or RAID configurations. Grouping drives together creates a larger logical unit, increases reliability, and enhances performance.

Storage pools are more flexible and can potentially include hundreds of disks. Storage pools allow you to use the physical disk space more efficiently. Mirrored storage pools can be resistant to disk failure.

RAID allows for storage to be shared between disks in ways that can improve reliability. However, RAID configurations are less flexible than storage pools and are not easily expanded.

Storage pools offer greater flexibility and ease of maintenance. Therefore, Seagate recommends storage pools over RAID.

Note: Disks that are configured for RAID cannot be used in storage pools.

RAID Types

RAID levels vary according to the number of hard drives, protection, and performance.

RAID 0 - Striped volume: Unallocated space on two or more drives combined into a single array. RAID 0 offers a small improvement in performance, but no data protection should a hard drive fail.

RAID 1 - Mirrored volume: Unallocated space on two drives is combined into a single array. The same data is simultaneously written to both drives. This provides a measure of data safety if a single drive fails. However, you lose 50% of the total disk capacity due mirroring the data.

RAID 5 - Striped volumes with distributed parity: Unallocated space on at least three hard drives is combined into a single array. RAID 5 offers improved performance and data protection. If a single drive fails, the data can be recovered. A RAID-5 volume requires space on at least three separate physical disks. There is one-third-space overhead for RAID-5 disks. For example, if you create a RAID-5 volume from three 1TB drives, the resulting RAID-5 volume will be 2TB.

.

Virtual Disks

Virtual disks can have one of the following storage layouts:

- **Simple**—Data is striped across the physical disks. This layout increases the speed of data access and maximizes storage capacity for the physical disks, but it does not offer fault tolerance.

- **Mirror**—Data is written on more than one physical disk. This method reduces capacity, but can protect the data from a single disk failure. Using five physical disks can protect the data form dual disk failures.

- **Parity**—Data with parity information is striped across the physical disks. The reduction in total storage capacity is less than a mirror layout. You need at least three physical disks to protect from a single disk failure. This method does not protect the data from multiple simultaneous disk failures.

A virtual disk can have one of the following provisioning systems:

- **Thin**—The virtual disk can grow with disk use. It claims space from the storage pool as needed.

- **Fixed**—The virtual disk is assigned a fixed amount of storage capacity. It requires specific action from an administrator to grow.

Create a storage pool

You can create a storage pool with physical hard drives that are unallocated, called the *primordial pool*.

1. Open Server Manager.

2. After Server Manager has polled the server storage, in the left menu, select **File and Storage Service**.

3. Under Volumes, select **Storage Pools**.

4. Select **Tasks > New Storage Pool**.

5. Use the New Storage Pool wizard to create a storage pool.

   When naming the pool, use a name short enough to fit in the Server Manager list.

After the storage pool is created, you can create a virtual disk to make the storage pool available for use.

Create a RAID volume

1. In the upper right of the Server Manager Dashboard, select **Tools > Disk Management**.

2. Right-click the disk you want to use and select **Convert to Dynamic Disk**.

3. Repeat for each unallocated volume to be used. There must be a minimum of three on three separate hard drives.

4. Right-click one of the unallocated volumes and select **New RAID-5 Volume**.

5. Use the New RAID-5 Volume wizard to create the volume

The time to complete the process depends on the total capacity. You can use the volume while it creates the RAID volume but performance might be affected.

Create a virtual disk

1. Open Server Manager.

2. After Server Manager has polled the server storage, in the left menu, select **File and Storage Service**.

3. Under Volumes, select **Storage Pools** and choose the storage pool you want to use for the virtual disk.

4. Select **Tasks > New Virtual Disk**.

5. Use the New Virtual Disk wizard to create a virtual disk.

   When naming the virtual disk, use a name short enough to fit in the Server Manager list.

A virtual disk must have a file system before it can be used by PCs on the network. For more information, see Volumes.

Add a hard drive to a storage pool

To add a hard drive to a storage pool, it must first be inserted into the server's enclosure. You cannot add USB or USM hard drives to storage pools.

1. In Server Manager, select **Storage Pools** under Volumes.

2. Right-click the storage pool that you want to expand and select **Add Physical Disk**.

   The available physical disks display.

3. Select the disk to add to the storage pool and click **OK**.

Important: You can view unallocated portions of disks that are added to storage pools in Disk Management. However, if an entire disk has been added to a storage pool, it is not be visible in Disk Management.

Extend a virtual disk

You can increase the size of a virtual disk.

1. In Server Manager, select **Storage Pools** under Volumes.

2. Select the storage pool that contains the virtual disk.

   The list of virtual disks displays.

3. Right-click the virtual disk that you want to expand and select **Extend Virtual Disk**.

4. Enter the new size and click **OK**.

Volumes

A volume is a logical storage space available to a PC. When the volume is allocated on the virtual disk, it is assigned a size, a drive letter, and a file system.

Using ReFS Versus NTFS

WSS 2012 has two types of file systems: Resilient File System (ReFS) and New Technology File System (NTFS). NTFS has been the principal file system for Windows implementations since 1993. ReFS is based on NTFS, but has been enhanced for storage applications.

ReFS offers the following functionality:

- Allows for very large files, volumes, and directories

- Allows for performance using data striping

- Supports disk scrubbing for recovery from latent disk errors

- Stores metadata, such as file attributes, with checksums to allow detection and correction of most types of disk corruption

- Supports copy-on-write to prevent data corruption from "torn" write tasks. The previous copy is not written over until the new write is complete.

- Uses B+ trees for performance with both small and large file structures

ReFS cannot be:

- Encrypted using Encrypting File System (EFS)

- Used on a boot drive, removable media, or drives that will be compressed

- Expanded after the volume is allocated

- Used for quota management

If you are using NTFS, you can expand or reduce the volume size.

Create a volume

To allocate a volume:

1. Open Server Manager.

2. After Server Manager has polled the server storage, in the left menu, select **File and Storage Service**.

3. Select **Disks** to display the virtual disks and unallocated physical disks.

4. Select the disk for the new volume.

   The system displays the volumes already defined on the disk.

5. Select **Tasks > New Volume**.

6. Use the New Volume wizard to create a volume.

Expand an NTFS volume

You can expand NTFS volumes.

1. Open Server Manager.

2. After Server Manager has polled the server storage, in the left menu, select **File and Storage Service**.

3. Select **Volumes** to display the volume list.

4. Right-click the volume to expand and select **Extend Volume**.

5. Enter the new size and click **OK**.

Shrink an NTFS volume

You can reduce the size of an NTFS volume.

1. In the upper right of the Server Manager Dashboard, select **Tools > Disk Management**.

2. Right-click the volume to reduce and select **Shrink Volume**.

3. Enter the amount of storage space to take away from the volume and click **Shrink**.

BitLocker drive encryption

BitLocker is a volume-level encryption service that protects data on hard drives that have been booted on a foreign operating system or another computer. When BitLocker is used on a data volume, the user is prompted for a password before being able to use its data. When it is used on the system volume, you unlock it using a password or an encrypted key on a USB drive.

You must add BitLocker as a feature to WSS 2012.

Add BitLocker

1. Open Server Manager and select **Local Server** in the left column.

2. Scroll to Roles and Features.

3. Select **Tasks > Add Roles and Features**.

4. Use the Add Roles and Features wizard to add BitLocker.

BitLocker is added as a feature to the target server. After restart, the Control Panel includes BitLocker Drive Encryption under the heading System and Security.

Enable BitLocker drive encryption on a data volume.

You can enable encryption on a volume if BitLocker is installed.

---

1. In the Control Panel, select **System and Security > BitLocker Drive Encryption**.

   A list of volumes with the notation BitLocker off appears.

2. Select the volume to encrypt and click **Turn on BitLocker**.

3. Choose the authentication method, and, if necessary, enter the password.

4. If you selected password protection, choose how to save it.

5. Choose what to encrypt.

   Keep in mind that even deleted files can be recovered by unauthorized users. If you have deleted files on the volume that should be protected, it is recommended that you encrypt the entire drive.

6. Click **Start**.

   A progress bar appears.

7. When finished, click **Close**.

Enable BitLocker drive encryption on the system volume

Adding BitLocker encryption to your system volume gives you greater security.

Before enabling BitLocker encryption on the system volume, you must change a policy:

1. Place your cursor in the upper or lower right corner of the desktop and click the **Search** tool.

2. In the Apps search window, type **gpedit.msc** and click the **gpedit.msc** icon.

3. In the left navigation panel, go to **Local Computer Policy > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives**.

4. Select **Require additional authentication at startup**.

5. If you are in the Extended tab at the bottom, select **Edit policy setting** to open the policy-editing window.

   If you are in the Standard tab at the bottom, the window automatically appears.

6. Select **Enabled**. If you cannot select it, select **Allow BitLocker without a compatible TPM**.

   You can enter a comment about the policy change.

7. Click **OK**.

8. Enable BitLocker data encryption for the system volume using the same steps provided for a data volume.

Unlock a volume

After a volume is encrypted, it must be unlocked after rebooting.

1. In the Control Panel, select **System and Security > BitLocker Drive Encryption**.

    A list of volumes displays. The locked volume has BitLocker on.

2. Select the volume and click **Unlock drive**.

3. Enter the password and click **Enter**.

You can use the Control Panel option Turn on auto-unlock to automatically unlock the volume if the Windows system drive is unlocked. To enable this option, the Windows system drive (C:) must be encrypted. If BitLocker is enabled on the Windows system drive, additional authentication is required during the boot process.

USB and USM Drives

USB Drives

If your Seagate server includes USB ports, USB hard drives and flash drives can be managed with the same tools as conventional disk drives.

It is strongly recommended that you do not add USB drives to volumes associated with internal drives. Removing a USB drive from such a volume can have unpredictable effects on the volume's data.

USM Drives

Your Seagate server might include a universal storage module (USM) slot that supports SATA II and SATA III hard drives for added storage. A USM drive is ideal for backing up data that you want to transport to a separate location or copy to another computer.

The volumes on the USM drive must be separate from the volumes on internal drives. **Seagate recommends that you do not add USM drives to volumes associated with the internal drives**.

4.   Shares

A *share* is a file folder that is available to users across the network. You can assign permissions and settings to a share to suit the security needs of different applications and organizations.

Shares can have shadow copies that are automatically added to a designated folder. You can use a shadow copy to recover deleted, overwritten, or modified files.

Two formats are available for a share file:

- **Server message block (SMB)**—Standard for Windows PCs and compatible with Mac and Linux.

- **Network file service (NFS)**—Typically used with UNIX or Linux-based PCs.

Share profiles

Server Manager simplifies the creation of shares by providing redefined share profiles:

- **SMB Share - Quick**—For Windows, Mac, and Linux computers sharing standard user data, such as documents and spreadsheets.

- **SMB Share - Advanced**—Adds options such as quotas on file space and defining default access permissions to the Quick profile. To use this profile, the File Server Resource Manager must be installed as a service on the server.

- **SMB Share - Applications**—Use if the volume is used with server applications that manage databases or virtual machines.

- **NFS Share - Quick**—For UNIX and Linux computers sharing standard user data, such as documents and spreadsheets.

- **NFS Share - Applications**—Use if the volume is used with server applications that manage databases or virtual machines.

Add a shared folder

1. In Server Manager, select **File and Storage Services**.

2. Select **Shares**.

3. Select **Tasks > New Share**.

4. Use the New Share wizard to create the shared folder.

   If you do not specify a directory, the share is added to the \Shares directory on the selected volume.

5. To complete the share creation, specify permissions for the folder and which users or groups can access it.

Install the File Server Resource Manager

To use the SMB Share Advanced profile, the File Server Resource Manager (FSRM) must be installed as a service on the server.

1. In Server Manager, select **All Servers** in the left column.

2. Right-click the server on which to enable the FSRM, and select **Add Roles and Features**.

3. Use the Add Roles and Features wizard to add the FSRM.

4. Under Installation Type, select **Role-based or feature-based installation** and click **Next**.

5. Select the server and click **Next**.

6. Under File and Storage Services > File and iSCSI Services, select **File Server Resource Manager**.

7. Complete the installation.

   You might be prompted to restart the server.

Enable shadow copies

Shadow copies allow you to automatically create copies of files in designated folders. Although convenient, you should not use shadow copies as an alternative to a true server backup. They are not stored off site, and they cannot be easily managed.

The shadow copy system can store up to 64 copies of a file.

1. In the Server Manager, select **Tools > Computer Management**.

2. In the left menu, under Storage, select **Disk Management**.

3. Right-click the volume to shadow and select **Properties**.

4. Select the Shadow Copies tab.

5. If the volume to shadow is not selected, click it.

6. Click **Settings** below the list of volumes.

   A dialog box displays.

7. Under **Storage Area**, specify the volume to store the shadow copies.

8. Under **Maximum Size**, specify the amount of space to allocate for shadow copies.

9. Click the **Schedule** button.

10. In the Schedule dialog box select the days and times to create the shadow copies.

11. Click **OK**.

The Volume Name Properties window appears and Under Next Run Time, shows when the system will next create shadow copies.

12. If a time is not listed, click **Enable** under the volume list.

13. To make shadow copies immediately, click **Create Now**.

14. Click **OK** to close the Volume Name Properties window.

Important: If you implement shadow copies on a clustered file server, ensure that the %SystemRoot% resolves to the same name on both the principal system and the failover system. If they do not match, shadow copies fail. For example, if %SystemRoot% is C:\Windows on one system and C:\Win on the other, the service that runs the shadow copy task can fail in the event of a system failover.

---

5.   NIC Teaming

No special configuration is required to use the server on multiple networks. When you connect each network adapter to its respective switch for the network, the server configures itself and the network traffic appropriately.

NIC Teaming

Seagate servers with more than one Ethernet port can take advantage of port aggregation, also known as NIC teaming.

Three configurations are available for NIC teaming:

• Switch independent teaming—Used when a switch does not support NIC teaming.

• Static teaming—Used for a switch that supports teaming but must be configured manually.

• LACP teaming—Used for a switch that supports LAN Aggregation Control Protocol (LACP). The switch does not require independent configuration.

For all NIC teams, the outbound and inbound traffic are distributed across the links in the team.

Traffic can be balanced across the ports in the following ways:

• **Hyper-V Port**—If the server uses Hyper-V virtual machines, each virtual machine has a separate MAC address and uses one server port exclusively. The server places all outbound traffic for the virtual machine on that port and the switch directs all in-bound traffic for that virtual machine to the same port.

• **Address Hashing**—The server creates a hash based on the address specified in each packet and assigns an outbound port based on the hash. This method load-balances outbound traffic. Balancing inbound traffic is not available for switch-independent teaming. All inbound traffic enters via one port.

• For static teaming, the switch's configuration determines which port to use for inbound traffic.

Configure a NIC team

To configure a NIC team, all Ethernet ports must be connected to the switch.

1. In Server Manager, select **Local Server** in the left column.

   The Properties table appears.

2. Click **NIC Teaming**.

3. In the NIC Teaming window, select **New Team** the TASKS menu.

4. Specify a name for the team and the network adapters to use.

5. Under the list of network adapters, click **Additional properties**.

6. Specify the teaming mode, the load-balancing mode, and whether both adapters are active.

7. Click **OK**.

   The new team appears the team table. The team may take a few seconds to resolve and become active.

6. iSCSI

Small Computer System Interface (SCSI) is a widely used protocol for controlling hard drives. Internet SCSI (iSCSI) uses the SCSI protocol on network volumes. In the iSCSI paradigm, the controller is known as the *initiator* and the network volume is the *target*.

Because SCSI offers greater speed than network file systems such as SMB and NFS, consider creating iSCSI targets for users with unique applications. For example, a PC on the network used for editing audio or video can take advantage of the faster protocol. Using an iSCSI target as opposed to standard direct-attached storage provides a centralized pool of storage that is easier to manage.

Professional versions of Windows have iSCSI built into the operating system. Third-party software is also available for Macs. When an initiator is paired with a target, the target volume must be formatted for the operating system, similar to standard SCSI hard drives. For example, a Windows initiator can format the target as NTFS and a Mac initiator can use HFS+.

WSS 2012 can also act as a name server for multiple iSCSI targets on the network. Targets register with the server, allowing initiators to connect to one device rather than search for multiple targets on the network. The WSS 2012 feature that manages iSCSI targets is called Internet Storage Name Service (iSNS). Your Seagate server can manage the naming for iSCSI targets created on its own pool of storage as well as other Windows and Linux servers on the network.

iSCSI Initiators

An iSCSI initiator is the server or computer that writes data to the iSCSI target. An initiator can search for and connect to a target on the network. It is also possible for a target to associate itself with an initiator.

An iSCSI initiator has an iSCSI Qualified Name (IQN) that can be useful when identifying the computer that is using the target. To find the initiator's IQN on Windows only:

- Open a Windows PowerShell command window and type the cmdlet **iscsisli**. The IQN displays inside square brackets as a prompt

  Or

- Search for **iSCSI Initiator** and launch it. The IQN is displayed as an initiator name on the iSCSI Initiator Properties Window Configuration tab:

  iqn.*nnnn-nn*.com.microsoft:seagate-*ddddd*

Create an iSCSI target

To create an iSCSI virtual disk and an iSCSI target on your server:

1. In Server Manager, select **File and Storage Services**.

2. Click **iSCSI**.

   A table of existing iSCSI virtual disks appears.

3. Select **Tasks > New iSCSI Virtual Disk**.

4. Use the New iSCSI Virtual Disk wizard to create the disk and target.

   You can also optionally add an initiator.

Important: Connecting an iSCSI target to more than one computer on the network and sharing files can cause file corruption. The one exception is a network that includes an iSCSI cluster server with file-sharing management. WSS 2012 cannot act as an iSCSI cluster server.

Add an Internet storage name server

The Internet storage name server (iSNS) provides discovery services for iSCSI initiators and targets on the network. Before you can start iSNS services, you must add it as a feature to WSS 2012:

1. In Server Manager, select **File and Storage Services**.

2. Select **Servers**.

3. In the server list, select the server on which to enable iSNS.

4. Select **TASKS > Add Roles and Features**.

5. Use the Add Roles and Features wizard to add iSNS.

6. Under Installation Type, select **Role-based or feature-based installation** and click **Next**.

7. Select the server and click **Next**.

8. Under File and Storage Services > File and iSCSI Services, select **Features**.

9. Select **iSNS Server service** and click **Next** to complete the installation.

10. If prompted, restart the server.

Register an iSCSI target with an iSNS server

Make sure that the iSNS service has been added as a feature WSS 2012.

1. Launch the PowerShell on the iSCSI target server.

2. Type:

   Set-WmiInstance -Namespace root\wmi -Class WT_iSNSServer -Arguments @{ServerName="Your_iSNS_ServerName"}

Where *Your_iSNS_ServerName* is the iSNS server name.

Important: Third-party or compatible NAS devices can have specific settings to join an iSCSI target to an iSNS server. Seagate NAS OS devices have a setting to join its iSCSI targets to an iSNS server.

Register an iSCSI initiator with an iSNS server (Windows only)

Make sure that the iSNS service has been added as a feature WSS 2012.

1. On your Windows computer, search for and launch **iSCSI initiator**.

2. On the Discovery tab, under iSNS servers, click **Add Server**.

3. Specify the IP address or DNS name of the iSNS server and click **OK**.

4. Click **Refresh**.

   The iSNS server is added to the list of iSNS servers.

5. Click **OK** to close the iSCSI Initiator Properties window.

7.   Backup

It is highly recommended that you backup your server at least once a day.

This chapter describes how to configure a backup using the Windows Server Backup utility. You can use other third-party applications that might provide additional features.

Server Backup for WSS 2012 has been improved so that administrators can spend less time managing the backup files. For example, after a complete server backup has been performed, subsequent automated backups are incremental, saving space and server resources.

To take full advantage of the Windows Server Backup utility, it is recommended that you connect a directly attached storage (DAS) device to the server as the backup destination. Using a DAS ensures that all files are efficiently backed up and give you earlier versions of files to choose from.

Choosing another server or NAS on the network as the backup destination limits your options, and you will not have a version history when searching for files in the backup.

Perform a one-time backup

1. In the Server Manager, select **Tools > Windows Server Backup**.

2. In the left navigation panel, select **Local Backup**.

3. In the right panel, select **Backup Once**.

4. Use the Backup Once wizard to set up the backup.

Note: Bare Metal Recovery is an option to include all the files needed to recover the operating system.

Set up a backup schedule

1. In the Server Manager, select **Tools > Windows Server Backup**.

2. In the left navigation panel, select **Local Backup**.

3. In the right panel, select **Backup Schedule**.

4. Use the Backup Schedule wizard to set up the backup.

   For the backup destination, a local disk gives you the best performance.

> **Note:** The first time you use a disk for backup, it is reformatted and all previous data on it is lost. The backup disk is also not visible to users in File Explorer.

Confirm a backup

You have two ways with the Windows Server Backup tool to check whether a backup has occurred:

1. In the left navigation panel, click **Windows Server Backup**.

   The state of the last backup is listed.

2. In the left navigation panel, click **Local Backup**.

   All backups for the last week appear in a table.

Recover files from a backup

These instructions apply to a full backup to a DAS:

1. In Server Manager, select **Tools > Windows Server Backup**.

2. In the left navigation panel, select **Local Backup**.

3. In the right panel, select **Recover**.

4. Use the Recovery wizard to recover files, folders, a Hyper-V machine state, a volume, an application, or a system state.

8. Active Directory

Important: Managing Active Directory requires a comprehensive understanding of Windows Server implementation. It is recommended that only administrators with experience make changes to the Active Directory.

Using Active Directory with Lightweight Directory Services

Your Seagate device can host an AD Lightweight Directory Services (LDS) service.

Install Active Directory Lightweight Directory Services

To use your Seagate device as an AD LDS server, you must first install AD LDS.

1. In the Server Manager, select **File and Storage Services**.

2. Select **Servers**.

3. In the server list, select the server on which to enable AD LDS.

4. Select **Tasks > Add Roles and Features**.

5. Use the Add Roles and Features wizard to add AD LDS.

6. Under Installation Type, select **Role-based or feature-based installation** and click **Next**.

7. Select the server and click **Next**.

8. In the left menu, select **Server Roles**.

9. Select **Active Directory Lightweight Directory Services** and click **Next**.

10. If a dialog box displays showing the list of tools and services that must be installed to use AD LDS, click **Add Features**.

11. Complete the installation.

12. Restart your server.

Configure Active Directory Lightweight Directory Services

After you have installed AD LDS, you must configure it.

1. In Server Manager, select **Tools > Active Directories Lightweight Directory Services Wizard**.

2. Use the wizard to configure AD LDS.

Using Active Directory with a Domain Controller

Your Seagate server can join an Active Directory domain controller as a member.

To add your server to an existing AD domain, you need the following information:

- Domain name

- Username and password for an administrative account in that domain

- Connection to the same network as the domain controller (LAN or WAN)

Join an Active Directory domain

To add the Seagate server to the AD domain:

1. In the Control Panel, click **System and Security**.

2. Select **System**.

3. To the right of the Computer Name, click **Change Settings**.

4. In the System Properties dialog box, click **Change**.

5. Under Member of, enter the domain name and click **OK**.

6. Enter the domain's administration credentials and click **OK**.

7. Confirm your selection at the prompts.

8. Restart your server.

Your server is now a member server of the Active Directory domain.

9. Distributed File Systems

A distributed file system (DFS) helps you maintain and share data on the network. Important functions such as data security, permissions, and accessibility are integrated into the DFS.

DFS Namespaces

During the course of a day, a user might need to access multiple files stored on many servers connected to your LAN or WAN. To find all the files spread about the network, the user hunts through a long list of shares.

Windows DFS Namespace (DFS-N) allows you to create a single virtual space that simplifies access for everyone. Although you configure DFS-N on the Seagate server, the shares can come from any server on the network.

Namespaces are visible to all users on the network. However, a user must have access rights to the shares to view and edit content.

DFS-N hierarchy

Before adding a namespace, you must understand the DFS-N hierarchy.

- Namespace server (in this case, the Seagate server)
- Namespace root (\\Seagate server\root)

   You can create multiple folders within a root folder.

- Folder seen by user (\\Seagate server\root\folder)

   Each folder in the root has its own target folder.

- Share mounted as a target folder (\\Seagate server\root\folder\target folder)

   The target folder is a share that has already been created. You can also create new shares.

Enable DFS namespaces

1. In Server Manager, select **File and Storage Services**.
2. Select **Servers**.
3. In the server list, select the server on which to enable DFS.
4. Select **Tasks > Add Roles and Features**.
5. Use the Add Roles and Features wizard to enable DFS.
6. Under Installation Type, select **Role-based or feature-based installation** and click **Next**.

7. Select the server and click **Next**.

8. In the left menu, select **Server Roles**.

9. Select **DFS Namespaces** and click **Next**.

10. If a dialog box displays showing the list of tools and services that must be installed to use DFS, click **Add Features**.

11. Complete the installation.

12. Restart your server.

Add a namespace

The namespace can be associated with a domain if the server has joined an Active Directory, or it can be a standalone server.

Associated with a single server, referred to as Stand-alone.

1. In Server Manager, select **Tools > DFS Management**.

2. Select **New Namespace** on the right.

3. In the New Namespace wizard, enter the name of your Seagate server—the host server for the namespace.

   It could be any server, because the namespace can include shares from multiple servers on the LAN or WAN.

4. Complete the instructions in the wizard to create the namespace.

Create a namespace folder

You can create folders to contain the target folders, such as folders based on a department or business.

1. In Sever Manager, select **Tools > DFS Management**.

2. On the left, expand the Namespaces list.

3. Right-click the namespace to use and select **New Folder**.

4. Type the name.

5. Right-click the folder and select **Add folder target**.

6. Browse for the share you want to add. You can also create a new share.

   Note: You can add a second share to a target folder to replicate data. Replication copies and updates files between the two shares. Your server must be a member of a domain for replication.

7. Create additional folders as needed.

DFS Replication

DFS replication (DFS-R) can improve bandwidth bottlenecks and enable users to spend their time more efficiently. DFS-R replicates data from a remote server to a local server on the LAN, providing users faster access to files. DFS-R also uses remote differential compression (RDC), which only replicates changes to a file rather than the entire file.

Note: Replication over the network is not the same as backing up a server. Replication, though convenient for avoiding WAN-related delays, is not a substitute for regular backups on an external hard drive or shared volume.

Enable DFS-R

1. In Server Manager, select **File and Storage Services**.

2. Select the server on which to enable DFS-R.

3. Select **Tasks > Add Roles and Features**.

4. Use the Add Roles and Features wizard to add DFS-R.

5. When the installation is complete, restart the system.

Add a replication group

1. In Server Manager, select **Tools > DFS Management**.

2. Right-click **Replication** and select **New Replication Group**.

3. Use the wizard to complete adding the group.

10. Seagate System Monitor

Seagate System monitor is a convenient tool for maintaining the health of your Seagate server. You can track the server's software, hardware, and hard drives.

Launch Seagate system monitor

1. In the Windows tool bar, click the Seagate icon.

2. Click a Seagate System monitor widget to get status information.

   A green light means that the system is working as expected. A red light indicates that immediate action is required.

11. Windows Recovery and Reset to Defaults

You must connect a mouse, keyboard, and monitor to the server to perform recovery and reset operations.

Recovery

The instructions below help you to recover WSS 2012. Use Windows Server Backup to recover data once the system recovery is complete.

Important: Disconnect the non-system hard drives from the enclosure before starting a recovery. Open the door to the enclosure and gently unplug the hard drives in slots 2-4.

---

1. Power down the server.

2. Connect a keyboard, video display, and mouse to the server.

3. Connect the USB key included with the your Seagate server.

4. On the rear of the unit, press the Recovery button (the recessed button marked with a pair of arrows) with a pointed object. Continue to press the Recovery button while you power on the server.

   The Recovery mode message displays.

5. After about 20 seconds, when the message **Starting recovery mode** displays, release the Recovery button.

6. Select **Windows Recovery**.

7. Select the keyboard layout.

8. Click **Troubleshoot**.

9. To recover from a backup, click **Advanced options**.

10. Select **System Image Recovery**.

    A message appears indicating that the backup cannot be found.

11. Unplug the USB key and connect your DAS with the server backup.

12. If your backup is located on a network volume, click **Advanced**, and then select **Search for a system image on the network**.

13. Enter the network path to the volume with the server backup.

14. Confirm that the backup located is correct and click **Next**.

15. Select which system image you want and click **Next**.

16. Click **System only**.

In most instances, the remaining options to format and repartition and install drivers are not necessary.

17. Click **Next**.

18. Review the settings and click **Finish**.

Reset Windows system hard drive and factory settings

1. Power down the server.

2. Connect a keyboard, video display, and mouse to the server.

3. Connect the USB key included with the your Seagate server.

4. On the rear of the unit, press the Recovery button (the recessed button marked with a pair of arrows) with a pointed object. Continue to press the Recovery button while you power on the server

The Recovery mode message displays.

5. After about 20 seconds, when the message **Starting recovery mode** displays, release the Recovery button.

6. Select **Seagate NAS Recovery**.

7. Select a recovery option and click **Start**.

8. Confirm and click **Next**.

12. Changing System Settings

Change the server name

Server names can be 1-15 characters long. The name can contain a period, but not as the first character. All characters are allowed except \/:*?"<>|.

1. Go to **Control Panel > System and Security**.

2. Select **System** and choose **See the name for this computer**.

3. Click **Change settings**.

4. Click **Change**, enter the new name, and click **OK**.

5. Restart the computer for the new name to take effect.

Update Windows

You can control how Windows applies system updates.

1. Go to **Control Panel > System and Security > Windows Update**.

2. Select **Turn on automatic updates**.

3. Click **Change settings**.

4. Under Important updates, select the update setting.

   Seagate recommends that you select **Download updates but let me choose whether to install them**.

   If you do not control when the updates are installed, the WSS might reboot at an inopportune moment.

5. To use the same setting for less important updates, select the check box next to **Give me recommended updates the same way I receive important updates**.

6. Click **OK**.

Shut down and Restart

To shut down or restart your server:

1. Move your mouse to the lower right corner of the Window Server 2012 desktop.

2. Click the Settings icon ( ).

3. In the pane, click the **Power** icon, and then select either **Shut down** or **Restart**.

13. Troubleshooting

How do I reset the Administrator password if it is lost?

You cannot recover a lost Administrator password. You must reinstall the Windows partition to reset the password.

Why can't I mount my iSCSI target on more than one location?

The iSCSI system works by emulating a SCSI hardware system, but instead of passing the disk commands from a SCSI disk controller to a SCSI disk, the iSCSI system passes the commands over a network to a virtual disk. If two iSCSI initiators interleave commands to the same disk, the disk can be corrupted. To prevent corruption, an iSCSI target can only be connected to one iSCSI initiator at once.

Why can't I use BitLocker on the C: Drive?

You can, but access to the C: drive needs to be authenticated at system boot time. This can be provided in the form of a manually entered password or a password on a USB drive. See chapter 3 for details.

Why can't I use this product with terminal services?

Windows licensing requires separate user licenses for each user accessing the system through terminal service.

Seagate Support

Contact Seagate Support at www.seagate.com/support