WILEY

SYBEX
A Wiley Brand

MCA: Windows Server Hybrid Administrator Study Guide: AZ-800 & AZ-801

Chapter 11: Configuring Storage

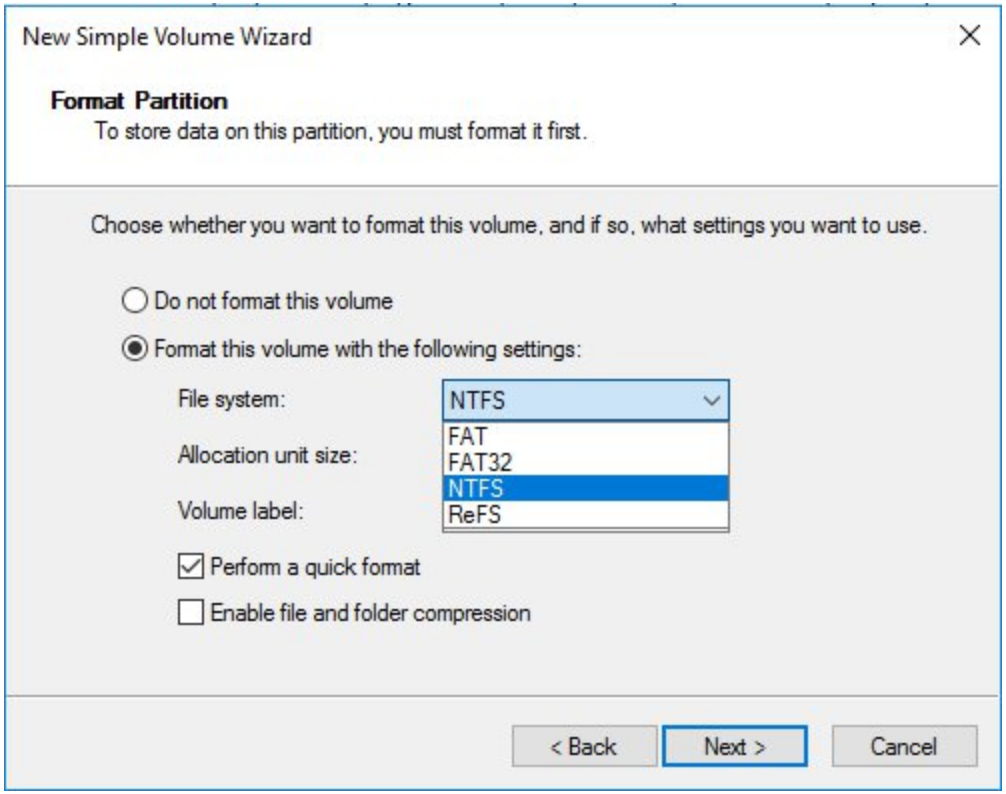
Understanding Filesystems

There are four file systems:

- FAT
- FAT32
- NTFS
- ReFS

- The Windows Server 2022 platform supports two file systems:
  - Windows NT File System (NTFS)
  - Resilient File System (ReFS)

Format Options on Windows Server 2022



Resilient File System (ReFS)

- Created to help Windows Server maximize the availability of data and online operation.
- ReFS allows the Windows Server 2022 system to continue to function despite some errors.
- ReFS uses data integrity.

ReFS Features

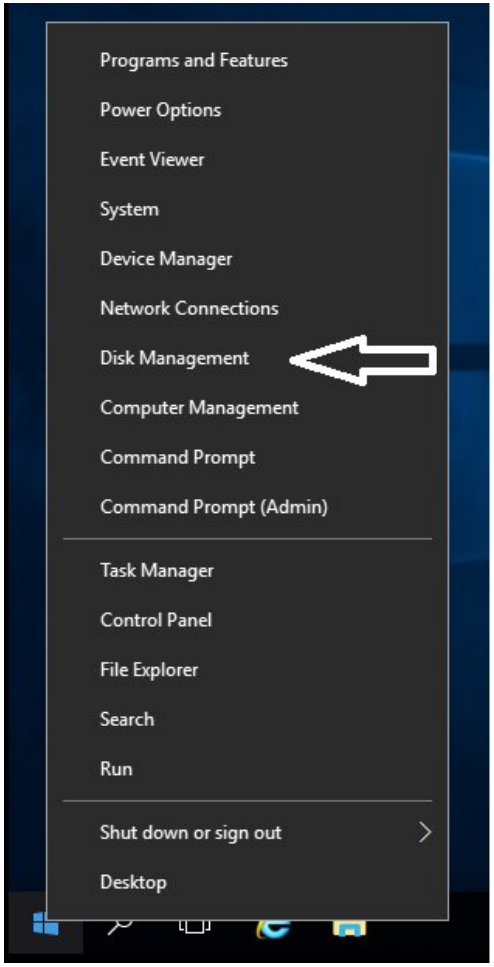
- Availability
- Scalability
- Robust Disk Updating
- Data Integrity
- Application Compatibility

NTFS Features

- Disk Quotas
- File System Encryption
- Dynamic Volumes
- Mounted Drives
- Remote Storage
- Self-Healing NTFS
- Security

Setting Up the NTFS Partition

- Disk Management
- Command Line Utility
  - CONVERT c: /fs:ntfs



Storage in Windows Server 2022

Disk Initialization Types:

- Master Boot Record (MBR)
- GUID Partition Table (GPT)

Disk Configuration Types:

- Basic Disks – divided into partitions
- Dynamic Disks – divided into volumes

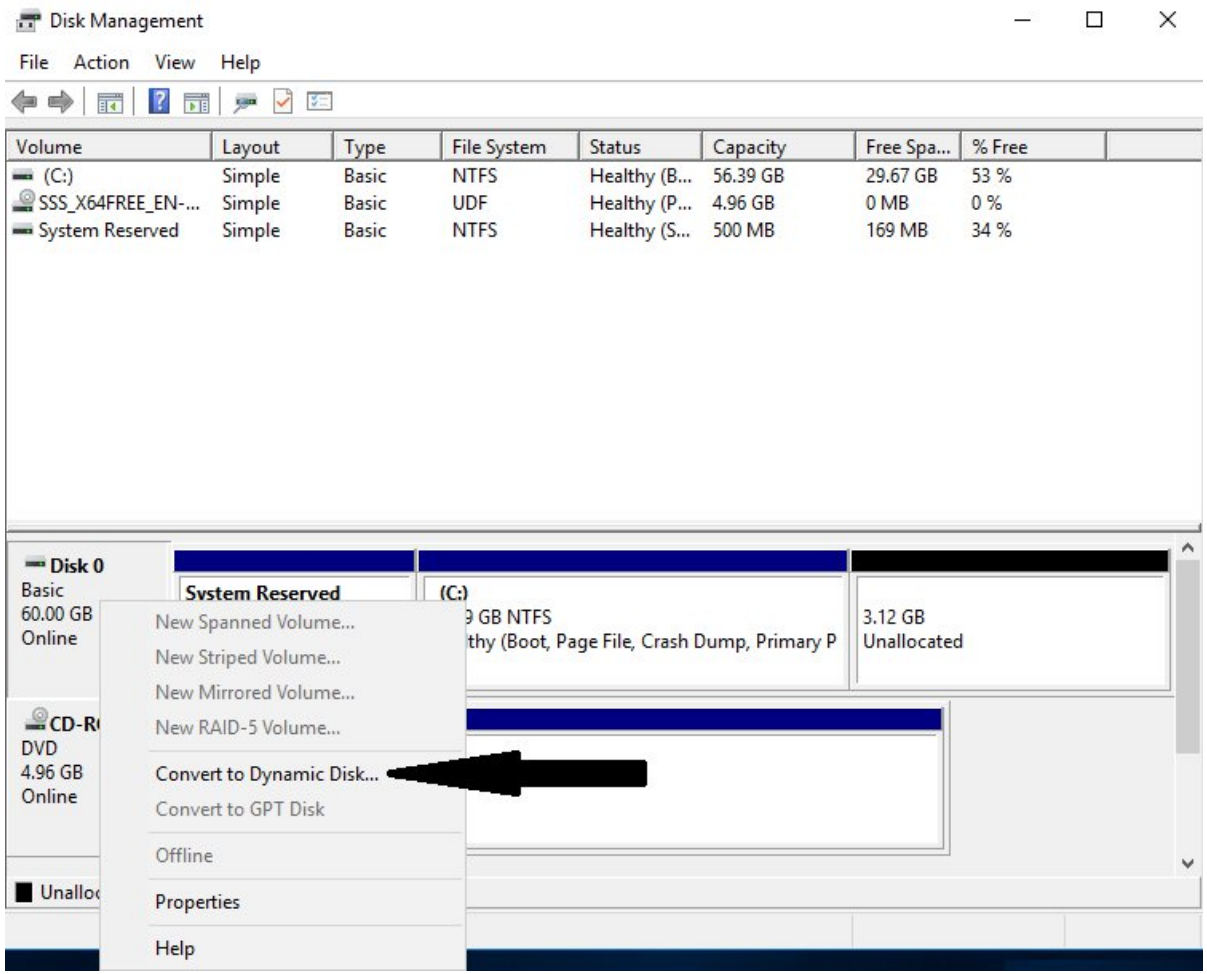
Basic Disk Actions:

- Formatting partitions.
- Marking partitions as active.
- Creating and deleting primary and extended partitions.
- Creating and deleting logical drives.
- Converting from a basic disk to a dynamic disk.

Dynamic Disk Actions:

- Creating and deleting simple, striped, spanned, mirrored, or RAID-5 volumes.
- Removing or breaking a mirrored volume.
- Extending simple or spanned volumes.
- Repairing mirrored or RAID-5 volumes.
- Converting from a dynamic disk to a basic disk after deleting all volumes.

Converting a Basic Disk to a Dynamic Disk



Managing Volumes

- A *volume set* is created from volumes that span multiple drives by using the free space from those drives to construct what will appear to be a single drive.
- Types:
  - Simple
  - Striped
  - Mirrored
  - RAID-5

Storage Spaces

- Virtualize storage by grouping disks into storage pools.
- Can be tuned into virtual disks called storage spaces.
- Managed by using:
  - Windows Storage Management API
  - Server Manager
  - Windows PowerShell
- Three types of resiliency: mirror, parity and simple (no resiliency).

Storage Spaces Advantages

- Availability
- Tiered Storage
- Delegation

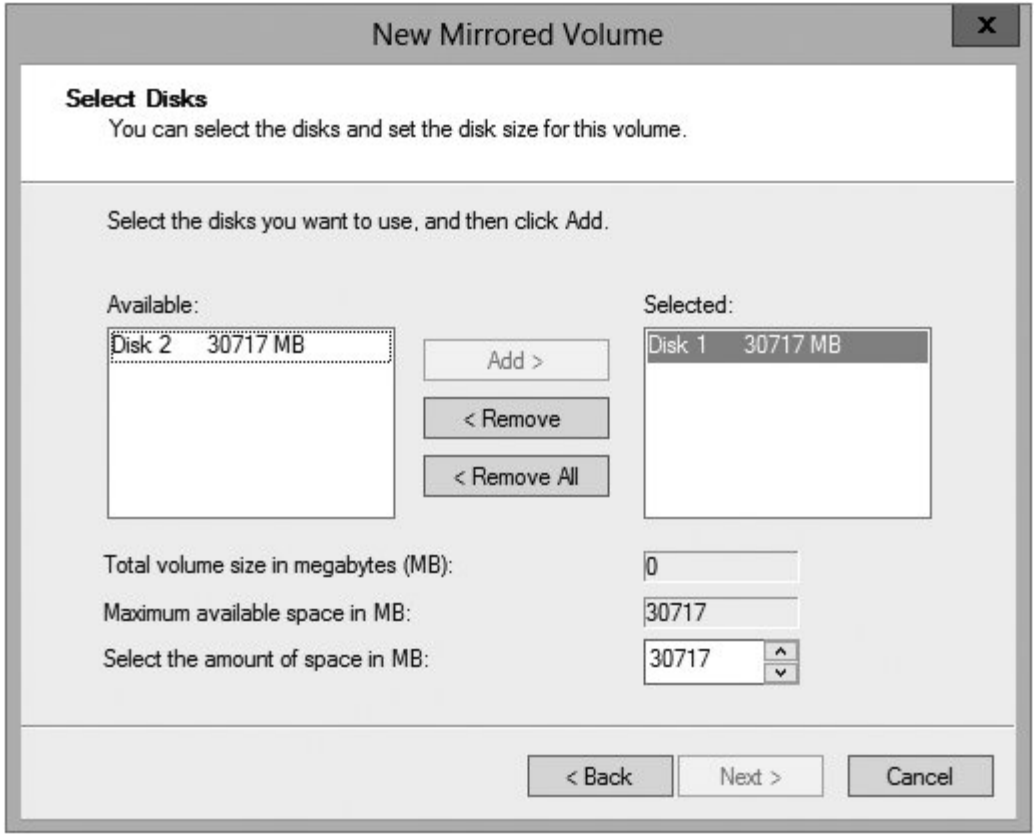
Redundant Array of Independent Disks (RAID) (1/2)

- RAID-0 (Disk Striping)
- RAID-1 (Disk Mirroring)
- RAID-5 Volume (Disk Striping with Parity)

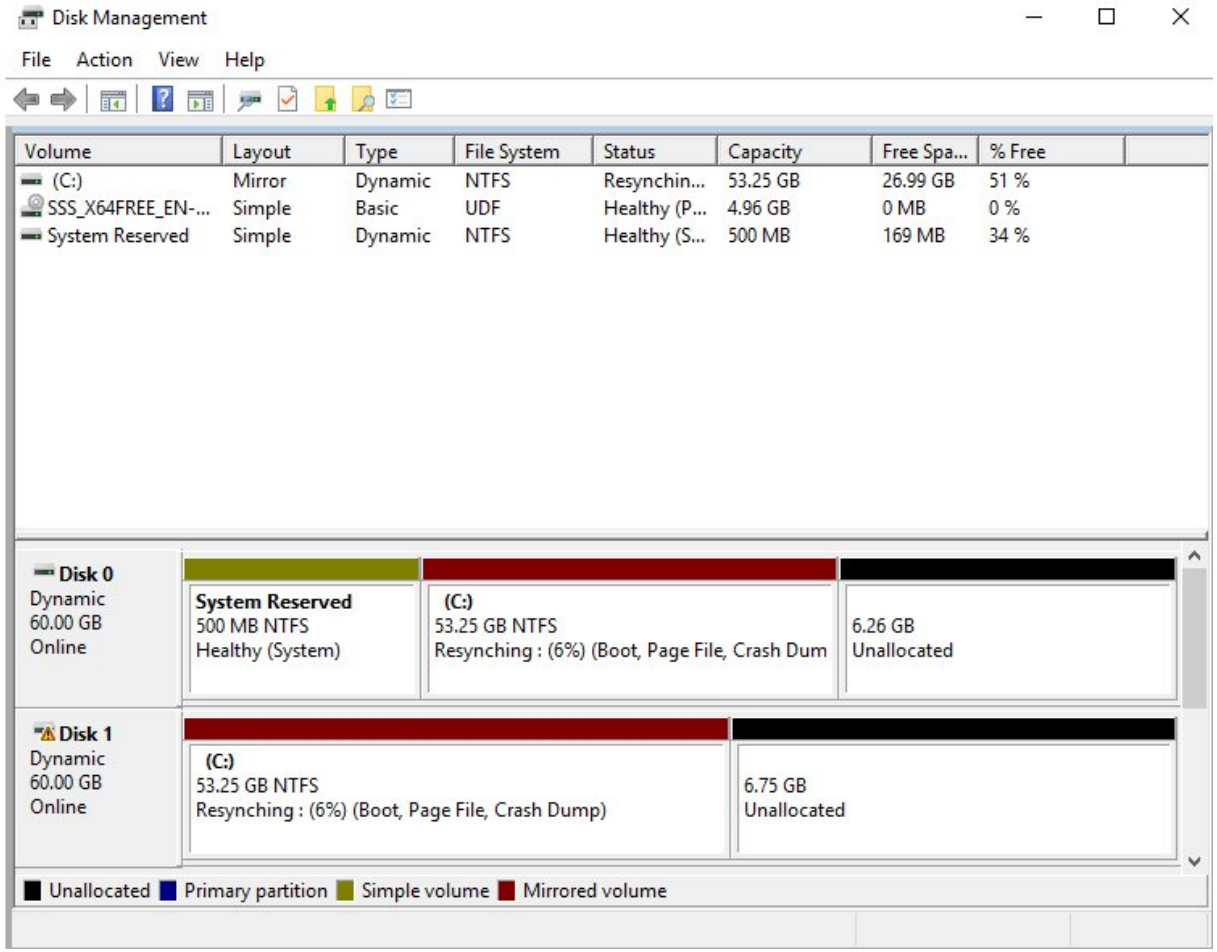
Redundant Array of Independent Disks (RAID) (2/2)

RAID Level	RAID Type	Fault Tolerant	Advantages	Minimum Number of Disks	Maximum Number of Disks
0	Disk striping	No	Fast reads and writes	2	32
1	Disk mirroring	Yes	Data redundancy and faster writes than RAID-5	2	2
5	Disk striping with parity	Yes	Data redundancy with less overhead and faster reads than RAID-1	3	32

Creating RAID Sets – New Mirrored Volume



Creating RAID Sets – New Mirrored Volume Created



Mount Points

- A *mount point* allows to configure a volume to be accessed from a folder on another existing disk.
- Using Disk Management, a mount point folder can be assigned to a drive instead of using a drive letter.
- Can be used on basic or dynamic volumes that are formatted with NTFS.

Microsoft Multipath I/O (MPIO)

- Windows Server 2022 supports the following load-balancing policies:
  - Failover
  - Failback
  - Round Robin
  - Round Robin with a Subset of Paths
  - Dynamic Least Queue Depth
  - Weighted Path

Installing Microsoft MPIO

Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-SFNGOK904VK

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

- [ ] Direct Play
- [ ] Enhanced Storage
- [ ] Failover Clustering
- [ ] Group Policy Management
- [ ] Host Guardian Hyper-V Support
- [ ] I/O Quality of Service
- [ ] IIS Hostable Web Core
- [ ] Internet Printing Client
- [ ] IP Address Management (IPAM) Server
- [ ] iSNS Server service
- [ ] LPR Port Monitor
- [ ] Management OData IIS Extension
- [ ] Media Foundation
- [■] Message Queuing (1 of 7 installed)
- [x] Multipath I/O
- [ ] MultiPoint Connector
- [ ] Network Load Balancing
- [ ] Peer Name Resolution Protocol
- [ ] Quality Windows Audio Video Experience

Description

Multipath I/O, along with the Microsoft Device Specific Module (DSM) or a third-party DSM, provides support for using multiple data paths to a storage device on Windows.

< Previous | Next > | Install | Cancel

Internet Small Computer System Interface (iSCSI)

- iSCSI is an interconnect protocol used to establish and manage a connection between a computer (initiator) and a storage device (target).
- Uses TCP port 3260.
- Each initiator is identified by its iSCSI Qualified Name (iqn).
- Alternative to Fibre Channel storage.

iSCSI - Continued

- iSCSI can use:
  - CHAP or MS-CHAP for authentication
  - IPsec for encryption

- Windows Server 2022 supports two different ways to initiate an iSCSI session.
  - Through the native Microsoft iSCSI software initiator that resides on Windows Server 2022.
  - Using a hardware iSCSI host bus adapter (HBA) that is installed in the computer.

Internet Storage Name Server (iSNS)

- Internet Storage Name Server (iSNS) allows for the central registration of an iSCSI environment because it automatically targets on the network.
- Help find available targets on a large iSCSI network.
- From command prompt:
  iscsicli addisnssserver server_name

Thin Provisioning and Trim

- Thin provisioning and trim can be useful features that allow organizations to get the most out of their storage arrays.
- Thin Provisioning – way of providing what is known as just-in-time allocations.
- Trim – automatically reclaims free space that is not being used. Windows Server 2022 provides standardized notifications that will alert administrators when certain storage thresholds are crossed.

Fibre Channel

- *Fibre Channel* storage devices are similar to iSCSI in that they both allow:
  - block-level access to their data sets
  - can provide MPIO policies with the proper hardware configurations
- Fibre Channel requires:
  - a Fibre Channel HBA
  - fiber-optic cables
  - Fibre Channel switches

Network Attached Storage

- A low-cost device for storing data and serving files through the use of an Ethernet LAN connection.
- Accesses data at the file level via a communication protocol such as NFS, CIFS, or even HTTP.
- Only setup required is an IP address and an Ethernet connection.

Virtual Disk Service (VDS)

- VDS is a set of application programming interfaces (APIs) that provide a centralized interface for managing all of the various storage devices.
- VDS includes two software providers: basic and dynamic.
- Windows Server 2022 storage management applications that use VDS:
  - Disk Management snap-in
  - DiskPart
  - DiskRAID

SYBEX
A Wiley Brand

DiskPart Commands

Administrator: Command Prompt - diskpart

```
DISKPART> help

Microsoft DiskPart

ACTIVE       - Mark the selected partition as active.
ADD          - Add a mirror to a simple volume.
ASSIGN       - Assign a drive letter or mount point to the selected volume.
ATTRIBUTES   - Manipulate volume or disk attributes.
ATTACH       - Attaches a virtual disk file.
AUTOMOUNT    - Enable and disable automatic mounting of basic volumes.
BREAK        - Break a mirror set.
CLEAN        - Clear the configuration information, or all information, off the
               disk.
COMPACT      - Attempts to reduce the physical size of the file.
CONVERT      - Convert between different disk formats.
CREATE       - Create a volume, partition or virtual disk.
DELETE       - Delete an object.
DETAIL       - Provide details about an object.
DETACH       - Detaches a virtual disk file.
EXIT         - Exit DiskPart.
EXTEND       - Extend a volume.
EXPAND       - Expands the maximum size available on a virtual disk.
FILESYSTEMS  - Display current and supported file systems on the volume.
FORMAT       - Format the volume or partition.
GPT          - Assign attributes to the selected GPT partition.
HELP         - Display a list of commands.
IMPORT       - Import a disk group.
INACTIVE     - Mark the selected partition as inactive.
LIST         - Display a list of objects.
MERGE        - Merges a child disk with its parents.
ONLINE       - Online an object that is currently marked as offline.
OFFLINE      - Offline an object that is currently marked as online.
RECOVER      - Refreshes the state of all disks in the selected pack.
               Attempts recovery on disks in the invalid pack, and
               resynchronizes mirrored volumes and RAID5 volumes
               that have stale plex or parity data.
REM          - Does nothing. This is used to comment scripts.
REMOVE       - Remove a drive letter or mount point assignment.
REPAIR       - Repair a RAID-5 volume with a failed member.
RESCAN       - Rescan the computer looking for disks and volumes.
RETAIN       - Place a retained partition under a simple volume.
SAN          - Display or set the SAN policy for the currently booted OS.
SELECT       - Shift the focus to an object.
SETID        - Change the partition type.
SHRINK       - Reduce the size of the selected volume.
UNIQUEID     - Displays or sets the GUID partition table (GPT) identifier or
               master boot record (MBR) signature of a disk.

DISKPART>
```

WILEY

Data Center Bridging (DCB)

- Requirements needed when deploying DCB through Windows Server 2022:
  - The Ethernet adapters installed must be DCB compatible.
  - The Hardware switches that are deployed to the infrastructure must also be DCB compatible.

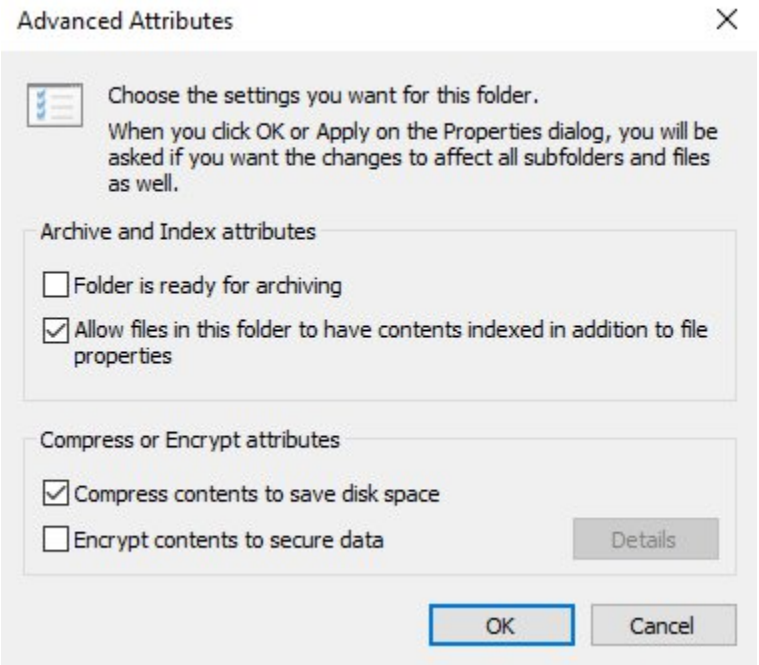
- DCB can be installed onto a Windows Server two ways:
  - Server Manager
  - Windows PowerShell

Server Message Block (SMB)

- A network-sharing protocol that allows Windows machines (either client- or server-based operating systems) that are running applications to read and write data to files.
- SMB runs on top of the network protocol that is being used on your corporate infrastructure.

NTFS Advantages Over FAT & FAT32

- Compression
- Quotas
- Encryption
- Security



Shared Permissions

- *Shared permissions* can be placed only on the folder and not on individual files.
- Files have the ability to inherit permissions from the parent folder.
- Shared permissions are additive.
- Deny permission overrides any group permission, and an individual permission overrides a group Deny.
- Shared permissions from lowest to highest are: Read, Change, Full Control, and Deny

SYBEX
A Wiley Brand

NTFS Security vs. Shared Permissions

Description	NTFS	Shared
Folder-level security.	Yes	Yes
File-level security.	Yes	No
In effect when local to the data.	Yes	No
In effect when remote to the data.	Yes	Yes
Permissions are additive.	Yes	Yes
Group Deny overrides all other group settings.	Yes	Yes
Individual settings override group settings.	Yes	Yes

WILEY

NTFS Security & Shared Permissions Work Together

Two basic rules of thumb:

- The local permission is the NTFS permission.
- The remote permission is the more restrictive set of permissions between NTFS and shared.

Shared permissions

StormWind Documents

NTFS security

Marketing	Sales	R&D
R	R	R

Local = ?

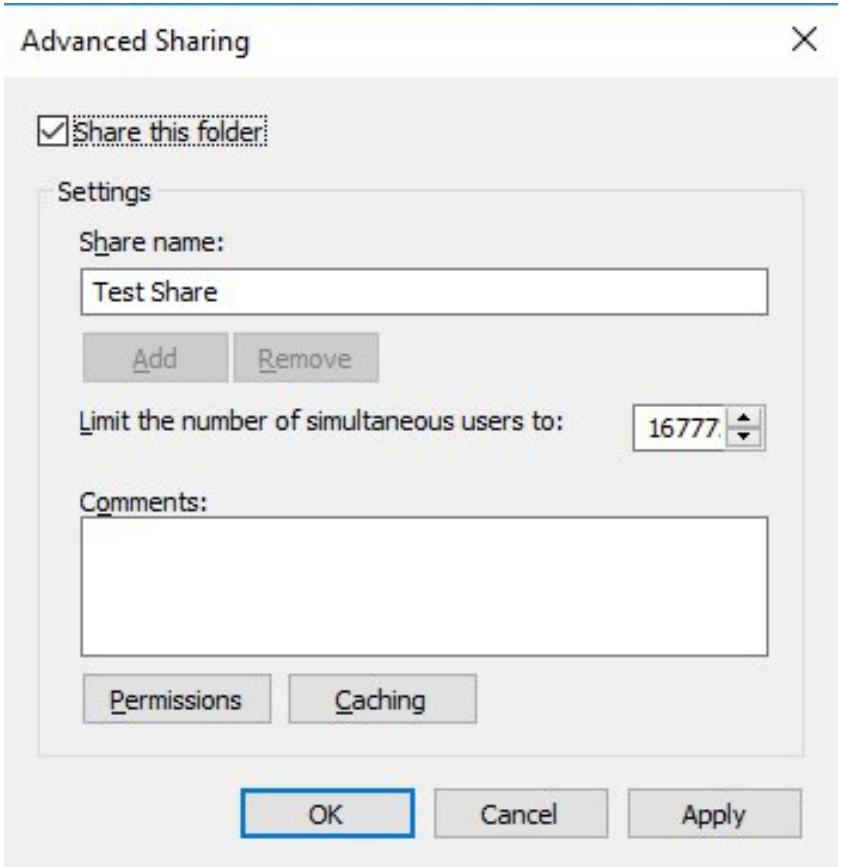
Remote = ?

Marketing	Sales	R&D
RX	R	FC

wpanek

Marketing
Sales
R&D

Configuring Shared and NTFS Settings – Advanced Sharing



NFS Shares

- NFS role service and feature gives the ability to integrate a Windows Server–based environment with Unix-based operating systems.
- With Windows Server 2022, can use an NFS share efficiently as an ESXi data store to house all of the guest virtual machines.
- With a Windows NFS file server, can configure file shares for use by multiple operating systems.

Disk Quotas

- *Disk quotas* give administrators the ability to limit how much storage space a user can have on a hard drive.
- Options:
  - Setting quotas by volume
  - Setting quotas by user
  - Specifying quota entries
  - Creating quota templates

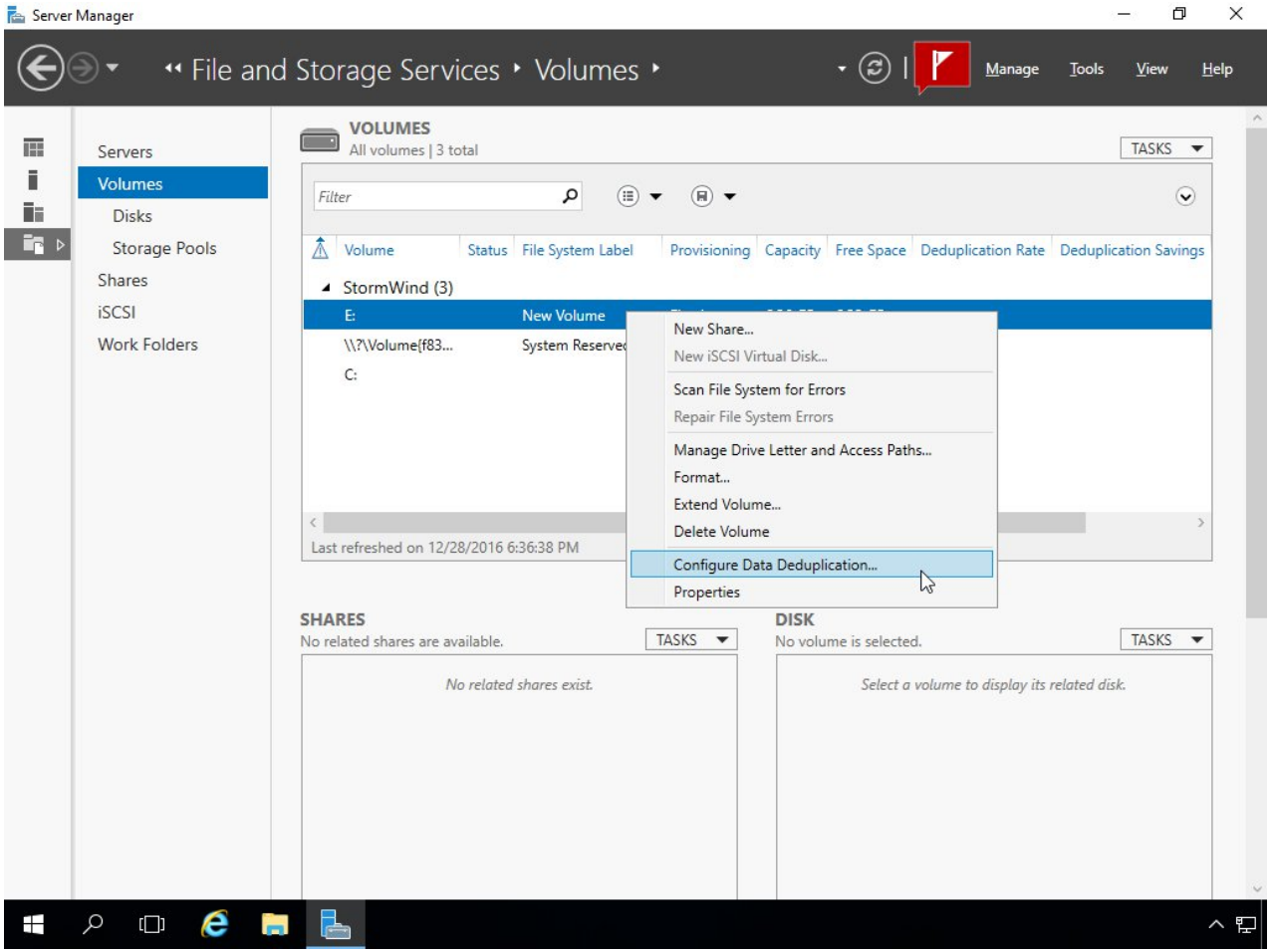
Data Duplication

- Data deduplication involves finding and removing duplicate data within the company network without compromising its integrity.
- Allows redundant copies of data chunks and then it references those multiple copies into a single copy.
- Replaced with markers that direct the computer system to the data blocks within the data store.

Enable Data Duplication

- Enable a volume for duplication and then the data is automatically optimized.
- After enabled, the volume will contain the following:
  - Optimized Files
  - Unoptimized Files
  - Chunk Store
  - Free Space
- Can install through Server Manager or Windows PowerShell.

Enabling Data Duplication



SYBEX
A Wiley Brand

Data Duplication Setup

New Volume (E:\) Deduplication Settings

New Volume (E:\)

Data deduplication: General purpose file server

Deduplicate files older than (in days): 3

Type the file extensions that you want to exclude from data deduplication, separating extensions with a comma. For example: doc,txt,png

Default file extensions to exclude: edb,jrs

Custom file extensions to exclude: .exe

To exclude selected folders (and any files contained in them) from data deduplication, click Add.

\test share

Add...

Remove

Set Deduplication Schedule...

OK Cancel Apply

WILEY

Monitoring Data Deduplication

After data duplication is installed and configured, an administrator will want to monitor the progress of the data duplication jobs.

To do this, run the following PowerShell commands (this command will show you the status of the duplication process);

- Get-DedupStatus
- Get-DedupVolume

File Server Resource Manager (FSRM)

- The File Server Resource Manager (FSRM) is a suite of tools that allows an administrator to place quotas on folders or volumes, filter file types, and create detailed storage reports.
- Allows administrators to control and manage the amount and type of data stored on your servers.

FSRM Features

Some of the advantages included with FSRM are as follows:

- Configure File Management Tasks
- Configure Quotas
- File Classification Infrastructure
- Configure File Screens
- Configure Reports

Installing the FSRM Role Service

Can install FSRM either by:

- Using Server Manager, go into Add Roles And Features and choose File And Storage Services ➢ File Services ➢ File Server Resource Manager.
- Using PowerShell (on next slide)

Installing the FSRM Role Service Using PowerShell

- To install FSRM using PowerShell, you use the following command:

```
Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools
```

SYBEX
A Wiley Brand

PowerShell Commands for FSRM

PowerShell cmdlet	Description
`Get-FsrmAutoQuota`	Gets auto-apply quotas on a server
`Get-FsrmClassification`	Gets the status of the running file classification
`Get-FsrmClassificationRule`	Gets classification rules
`Get-FsrmFileGroup`	Gets file groups
`Get-FsrmFileScreen`	Gets file screens
`Get-FsrmFileScreenException`	Gets file screen exceptions
`Get-FsrmQuota`	Gets quotas on the server
`Get-FsrmSetting`	Gets the current FSRM settings
`Get-FsrmStorageReport`	Gets storage reports
`New-FsrmAutoQuota`	Creates an auto-apply quota
`New-FsrmFileGroup`	Creates a file group
`New-FsrmFileScreen`	Creates a file screen
`New-FsrmQuota`	Creates an FSRM quota
`New-FsrmQuotaTemplate`	Creates a quota template
`Remove-FsrmClassificationRule`	Removes classification rules
`Remove-FsrmFileScreen`	Removes a file screen
`Remove-FsrmQuota`	Removes an FSRM quota from the server
`Set-FsrmFileScreen`	Changes the configuration settings of a file screen
`Set-FsrmQuota`	Changes the configuration settings for an FSRM quota

WILEY

BitLocker Drive Encryption

- Encrypts the entire system drive. Files added are encrypted automatically, and files moved from this drive to another drive or computers are decrypted automatically.
- Windows Server 2022 includes BitLocker Drive Encryption, and only the operating system drive (usually C:) or internal hard drives can be encrypted with BitLocker.
- Uses a Trusted Platform Module (TPM) version 1.2 or higher to store the security key
- Alternately can store the key on a removable USB drive
- Requires two partitions, both formatted with NTFS. One for the system partition that will be encrypted. The other partition as the active partition. used to start the computer; which remains unencrypted
- If TPM discovers a potential security risk, such as a disk error, or changes made to BIOS, hardware, system files, or startup components, the system drive will remain locked until you enter the 48-digit recovery password or plug in a USB drive with a recovery key as a recovery agent.

Features of BitLocker

- BitLocker Provisioning
- Used Disk Space–Only Encryption
- Standard User PIN and Password Change
- Network Unlock
- Support for Encrypted Hard Drives for Windows

EFS Drive Encryption

- Encrypting is simple; just select a check box in the file or folder's properties to turn it on.
- Have control over who can read the files.
- Files are encrypted when you close them but are automatically ready to use when you open them.
- If you change your mind about encrypting a file, clear the check box in the file's properties.

Using the Cipher Command

- Cipher is a command-line utility that allows you to change and/or configure EFS.
- Administrators can:
  - Decrypt files by running **Cipher.exe** in the Command Prompt window (advanced users).
  - Use Cipher to modify an EFS-encrypted file.
  - Use Cipher to import EFS certificates and keys.
  - Use Cipher to back up EFS certificates and keys.

Cipher Switches

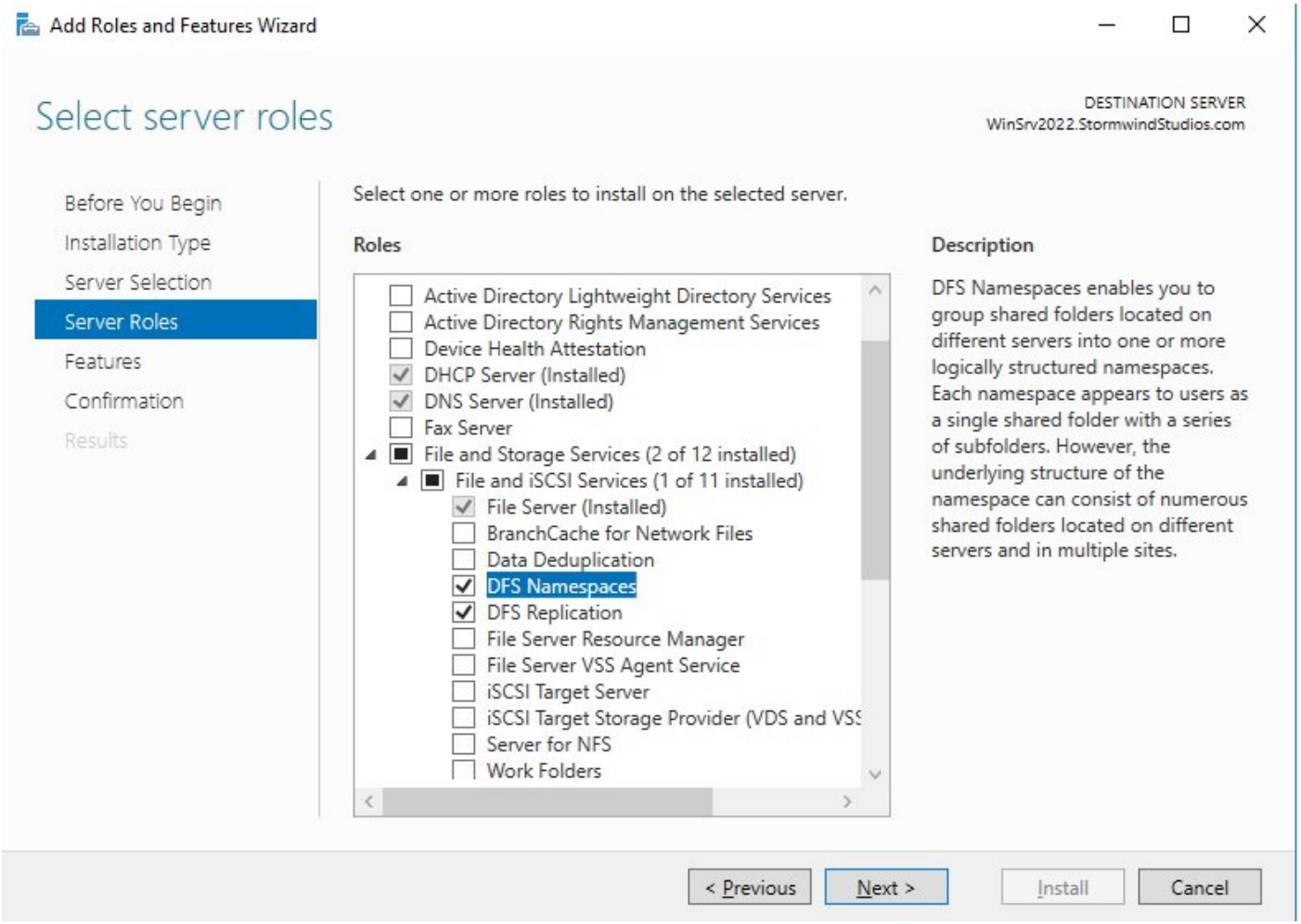
Cipher switch	Description
/e	This switch allows an administrator to encrypt specified folders. With this folder encrypted, any files added to this folder will automatically be encrypted.
/d	This switch allows an administrator to decrypt specified folders.
/s: dir	By using this switch, the operation you are running will be performed in the specified folder and all subfolders.
/i	By default, when an error occurs, Cipher automatically halts. By using this switch, Cipher will continue to operate even after errors occur.
/f	The force switch (/f) will encrypt or decrypt all of the specified objects, even if the files have been modified by using encryption previously. Cipher, by default, does not touch files that have been encrypted or decrypted previously.
/q	This switch shows you a report about the most critical information of the EFS object.
/h	Normally, system or hidden files are not touched by encryption. By using this switch, you can display files with hidden or system attributes.
/k	This switch will create a new file encryption key based on the user currently running the Cipher command.
/?	This shows the Cipher help command.

Distributed File System (DFS)

Distributed File System (DFS) in Windows Server 2022 offers a simplified way for users to access geographically dispersed files.

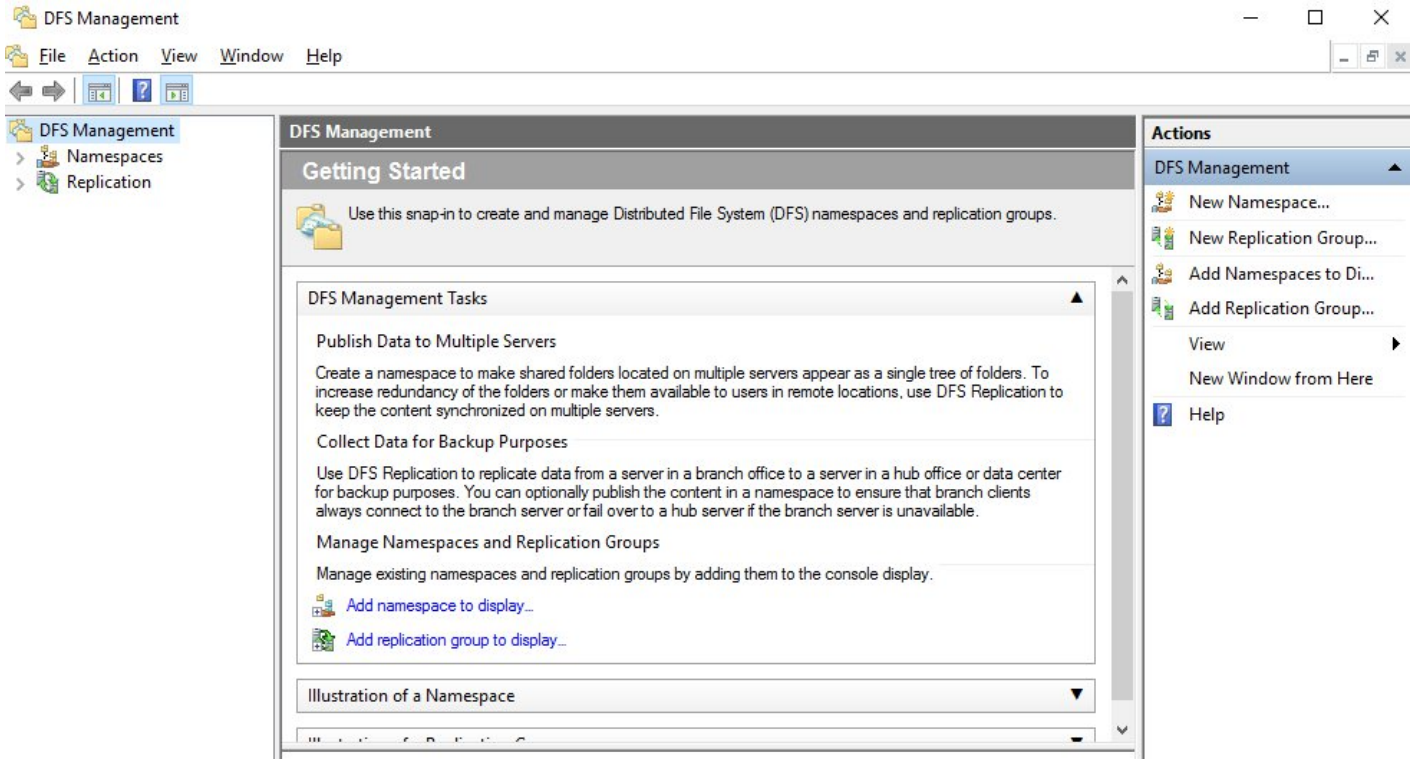
- Advantages of DFS
  - Simplified Data Migration
  - Security Integration
  - Access-Based Enumeration (ABE)
- Types of DFS
  - DFS Replication
  - DFS Namespaces

Installing DFS Namespace – Select Server Role



SYBEX
A Wiley Brand

DFS Management Console



WILEY

Database Cloning

- Windows Server 2022 includes a new DFS database cloning function. This feature allows you to accelerate replication when creating folders, servers, or recovery systems.
- Use the PowerShell `Export-DfsrClone` cmdlet to export the volume that contains the DFS database and configuration .xml file settings.
- Then use the PowerShell `Import-DfsrClone` cmdlet to import the data to a specific volume.

Recovering a DFS Database

- DFS database recovery is a feature that allows DFS to detect a corrupted database, thus allowing DFS to rebuild the database automatically and continue with normal operations of DFS replication.
- DFS uses local files and an update sequence number (USN) to fix a corrupt database, allowing for no loss of data.

Optimizing DFS

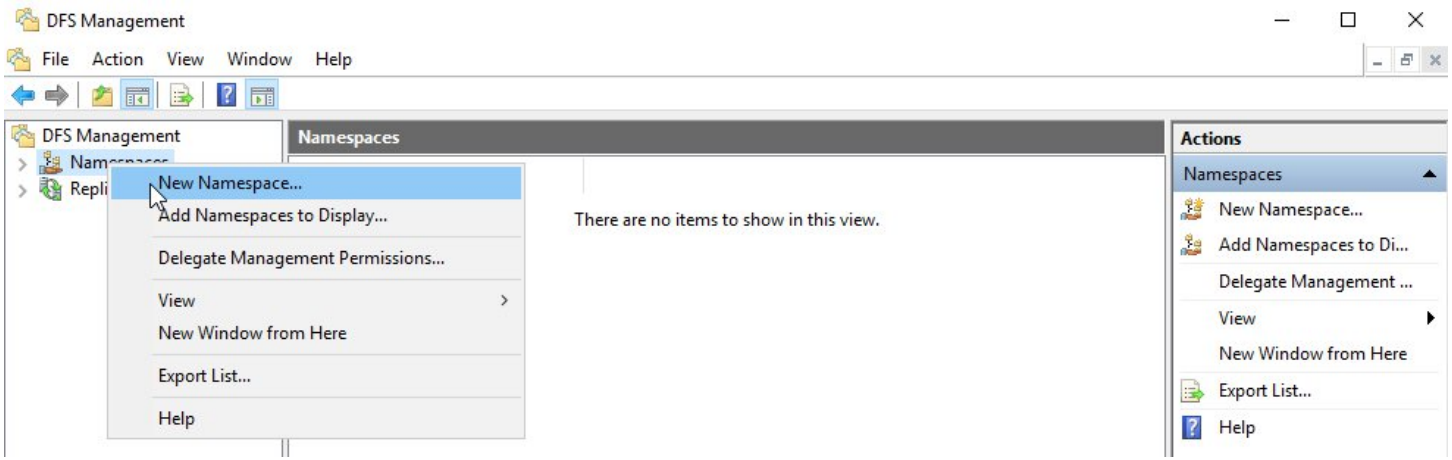
- DFS allows you to configure variable file staging sizes on individual DFS servers.
- This allows you to:
  - set a minimum file size for a file to stage.
  - increases the staging size of files.
  - and that in turn, increases the performance of the replication.

Remote Differential Compression (RDC)

- RDC is a group of application programming interfaces (APIs) that programs can use to determine whether files have changed. Once RDC determines that there has been a change, RDC then helps to detect which portions of the files contain the changes.
- RDC has the ability to detect insertions, removals, and rearrangements of data in files.

SYBEX
A Wiley Brand

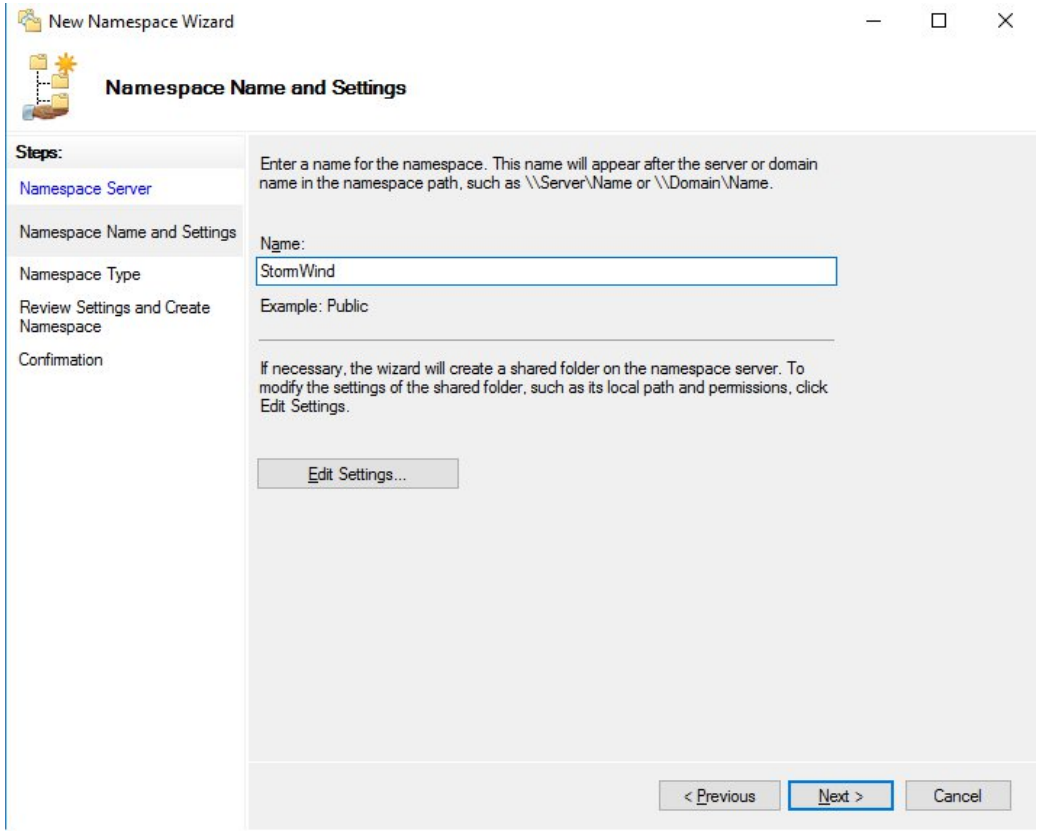
Setting up a DFS Namespace – Adding a Namespace (1/2)



WILEY

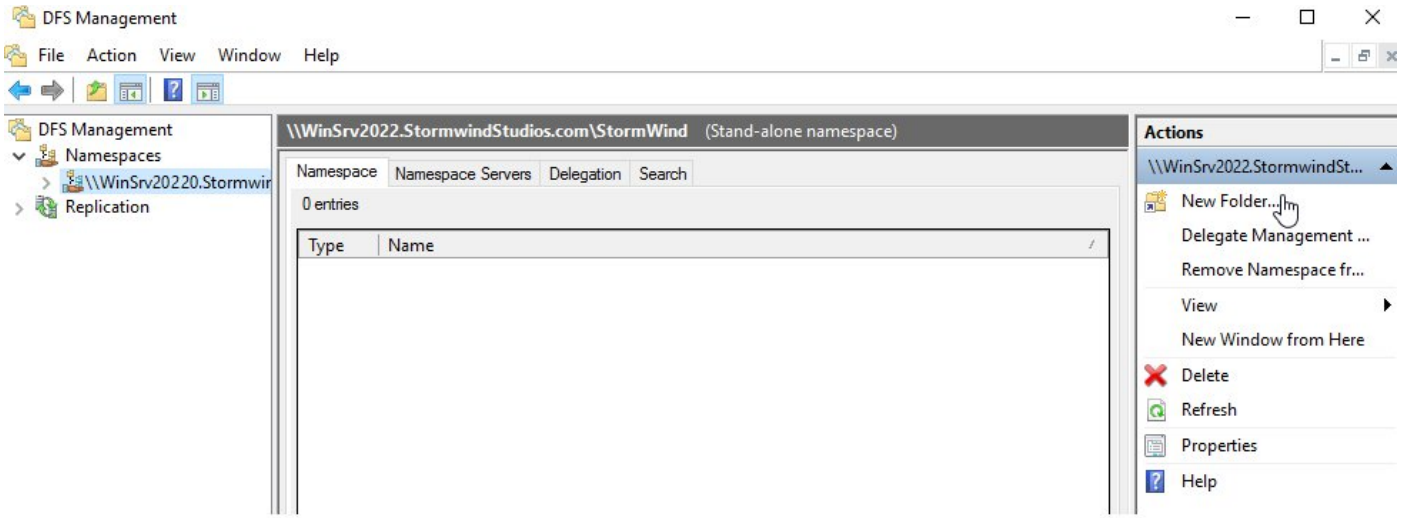
SYBEX
A Wiley Brand

Setting up a DFS Namespace – Adding a Namespace (2/2)

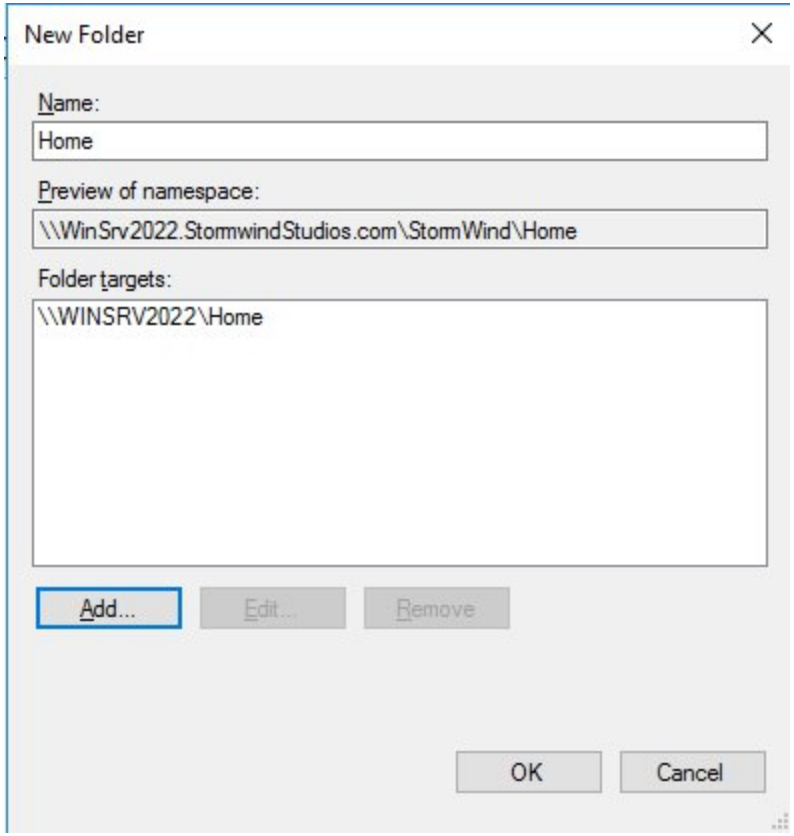


WILEY

Setting up a DFS Namespace – New Folder (1/2)



Setting up a DFS Namespace – New Folder (2/2)



Configure Network File System (NFS) Data Store

- The NFS role service and feature sets gives IT administrators the ability to integrate a Windows Server-based environment with Unix-based operating systems.
- With a Windows NFS file server, you can configure file shares for use by multiple operating systems.
- Windows Server 2022 enables you to integrate with platforms such as ESXi. ESXi is VMware's exclusive operating system–independent hypervisor.

Configure BranchCache

- BranchCache allows an organization with slower links between offices to cache data so that downloads between offices do not have to occur each time a file is accessed.
- BranchCache has two types of configurations:
  - Distributed Cache Mode – all Windows client machines cache the files locally on the client machines.
  - Hosted Mode – the cache files are cached on a local (within the site) Windows Server 2022 machine.

SYBEX
A Wiley Brand

Distributed Cache Mode Requirements

- The hosted cached server running Windows Server 2022 is not required at the branch office.
- The client machines must be running Windows 7 or above (except for home versions).
- Client machines download the data files from the content servers at the main office and then become the local cache servers.
- Client computers running Windows 7 Enterprise or higher (from versions listed above) have BranchCache installed by default.

WILEY

Hosted Mode Requirements

- Must first set up a Windows Server 2022 hosted cached server at the main and branch offices.
- Need to be running Windows 7 or above (except for home versions) at the branch offices.
- Client machines download the data from the main cache server and then the hosted cache server at the branch office obtains a copy of the downloaded data for other users to access.
- Your cache server must obtain a server certificate.

SYBEX
A Wiley Brand

Installing BranchCache

Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-SFNGOK904VK

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

- [ ] .NET Framework 3.5 Features
- [■] .NET Framework 4.6 Features (4 of 7 installed)
- [ ] Background Intelligent Transfer Service (BITS)
- [ ] BitLocker Drive Encryption
- [ ] BitLocker Network Unlock
- [x] BranchCache
- [ ] Client for NFS
- [x] Containers (Installed)
- [ ] Data Center Bridging
- [ ] Direct Play
- [ ] Enhanced Storage
- [x] Failover Clustering (Installed)
- [x] Group Policy Management (Installed)
- [ ] Host Guardian Hyper-V Support
- [ ] I/O Quality of Service
- [ ] IIS Hostable Web Core
- [ ] Internet Printing Client
- [ ] IP Address Management (IPAM) Server
- [ ] iSNS Server service

Description

BranchCache installs the services required to configure this computer as either a hosted cache server or a BranchCache-enabled content server. If you are deploying a content server, it must also be configured as either a Hypertext Transfer Protocol (HTTP) web server or a Background Intelligent Transfer Service (BITS)-based application server. To deploy a BranchCache-enabled file server, use the Add Roles Wizard to install the File Services server role with the File Server and BranchCache for network files role services.

< Previous | Next > | Install | Cancel

WILEY

PowerShell Cmdlets for BranchCache

Cmdlet	Description
`Add-BCDataCacheExtension`	Increases the amount of cache storage space that is available on a hosted cache server by adding a new cache file
`Clear-BCCache`	Deletes all data in all data and hash files
`Disable-BC`	Disables the BranchCache service
`Disable-BCDowngrading`	Disables downgrading so that client computers that are running Windows 10 do not request Windows 7/8 specific versions of content information from content servers
`Enable-BCDistributed`	Enables BranchCache and configures a computer to operate in distributed cache mode
`Enable-BCHostedClient`	Configures BranchCache to operate in hosted cache client mode
`Enable-BCHostedServer`	Configures BranchCache to operate in hosted cache server mode
`Enable-BCLocal`	Enables the BranchCache service in local caching mode
`Export-BCCachePackage`	Exports a cache package
`Export-BCSecretKey`	Exports a secret key to a file
`Get-BCClientConfiguration`	Gets the current BranchCache client computer settings
`Get-BCContentServerConfiguration`	Gets the current BranchCache content server settings
`Get-BCDataCache`	Gets the BranchCache data cache
`Get-BCStatus`	Gets a set of objects that provide BranchCache status and configuration information
`Import-BCCachePackage`	Imports a cache package into BranchCache
`Import-BCSecretKey`	Imports the cryptographic key that BranchCache uses for generating segment secrets
`Set-BCAuthentication`	Specifies the BranchCache computer authentication mode
`Set-BCCache`	Modifies the cache file configuration
`Set-BCSecretKey`	Sets the cryptographic key used in the generation of segment secrets

Enhanced Features in Windows Server 2022 BranchCache

- Office size and the number of branch offices are not limited.
- There are no requirements for a Group Policy object (GPO) for each office location, steamlining deployment.
- Client computer configuration is easy.
- BranchCache is deeply integrated with the Windows file server.
- Duplicate content is stored and downloaded only once.
- Small changes to large files produce bandwidth savings.
- Offline content creation improves performance.
- Cache encryption is enabled automatically.