Module 3: Implement enterprise storage solutions

Enterprise storage design is no longer just a capacity discussion. Modern environments must balance performance, resiliency, and operational simplicity while meeting security requirements for data access and transport. Windows Server 2022 and Windows Server 2025 both provide strong foundations for enterprise storage, and Windows Server 2025 adds notable enhancements in storage performance and modernization—particularly around high-performance NVMe storage paths, software-defined storage improvements, and modern SAN transports such as NVMe over Fabrics (NVMe-oF).

This module explains how to choose and implement enterprise storage approaches such as DAS, NAS, and SAN, and how to deploy file sharing services using SMB and NFS. The module also incorporates the Windows Server 2025 security posture for file services, especially SMB hardening defaults—and explains how hybrid patterns (for example, Azure File Sync and Azure File Sync) can complement enterprise file server solutions when organizations need tiering, multi-site access, or cloud-based recovery options.

> **Important update for Windows Server 2025:** Some legacy components are removed. In particular, iSNS is no longer available in Windows Server 2025, so discovery and management patterns should rely on modern alternatives (target portals, vendor SAN tooling, and standardized iSCSI/NVMe-oF practices).

SAMPLE

By completing this module, you'll achieve the knowledge and skills to:

- Describe DAS, NAS, and SAN.
- Compare Fibre Channel, iSCSI, and FcoE.
- Explain how to use iSNS, DCB, and MPIO.
- Configure sharing in Windows Server.

Lesson 1: Overview of direct-attached storage, network-attached storage, and storage area networks

For organizations with relatively few file servers, using DAS is a viable option. However, for larger organizations, and certainly for enterprise-level organizations, use if NAS and implementation of SANs is very likely. In this lesson, you'll learn about these fundamental storage decisions.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe DAS, NAS, and SANs.
- Compare block-level storage and file-level storage.

What is DAS?

DAS, as the name suggests, directly attaches to a file server or is installed in a server computer's chassis. All servers contain at least some DAS, if only the disk that's partitioned for startup and the operating system (OS).

> **Note:** These partitions are referred to as the System and Boot partitions, respectively.

There are several types of disks that you can attach locally, including Serial ATA (SATA), serial attached SCSI (SAS), and solid-state drive (SSD). For small deployments, adding additional DAS to servers isn't uncommon, regardless of whether the storage is internal or external.

> **Note:** It's common to add external storage to file servers and connect using a universal serial bus (USB).

Advantages of DAS

The main advantage of using DAS is simplicity. DAS connects to the server computer through a host bus adapter (HBA) or USB, so there aren't any complex network components to implement and configure.

It's also true that DAS is considerably less expensive to implement than network-connected storage solutions, partly because DAS requires fewer components to implement. However, it's also because the skills required to implement DAS are widely understood and don't require a specialist. Typically, you simply attach a new disk, and then Windows Server recognizes that disk and prompts you to configure partitioning and volumes on the disk.

SAMPLE

Disadvantages of DAS

A significant disadvantage of DAS is that the server computer itself becomes a single point of failure. If the server is unavailable, so is its attached storage.

Also, when adding additional disks, you must have physical access to the server. With servers increasingly being managed remotely from datacenters, this physical access can be problematic.

What is NAS?

With NAS, you attach your storage to a dedicated and network-connected storage device. In other words, the storage isn't connected to a physical server computer but can be made available to one or several server computers.

NAS supports two solutions:

- A low-end network appliance that supports only NAS.
- An enterprise network appliance that not only supports NAS, but which you also, or alternatively, configure to support SAN.

A NAS appliance has a dedicated OS that's tasked solely with providing access to the storage from the network servers configured to use it.

> **Note:** Windows Storage Server, a feature of Windows Server, is an example of NAS software.

After you physically deploy your NAS appliance and connect it to your network, you'll need to configure it and make the storage available. Typically, you must connect to the appliance across the network, as these devices tend not to have screens or keyboards for local access. You'll then create the necessary shares to enable access to the storage that connects to the appliance.

> **Tip:** NAS devices usually use file-level access over protocols such as Common Internet File System (CIFS), Server Message Block (SMB), and Network File System (NFS).

SAMPLE

Advantages of NAS

NAS is ideal when you require fast storage access at relatively low cost. NAS offers performance benefits that DAS doesn't because the storage appliance manages file access on behalf of your servers. The following list summarizes the advantages of using NAS versus DAS:

- NAS is less expensive to implement than SAN solutions.
- NAS typically supports larger capacities than DAS, so you can make more storage available.
- NAS appliances support Redundant Array of Independent Disks (RAID) configurations to provide for higher throughput and/or storage high availability.
- NAS provides centralization of storage, which is beneficial because:
  - Files aren't distributed across file servers, but rather in one place.
  - You can centrally manage your storage so there's no need to connect to multiple file servers to manage file shares.
- NAS appliances can be accessed from almost any OS, so it's possible to configure storage that both Linux and Windows Server users can access at the same time.
- NAS is typically available as a Plug and Play (PNP) solution, which makes it much easier to deploy and provision than SAN solutions.

Disadvantages of NAS

NAS is an obvious improvement over DAS in most, if not all, respects. However, that's not the case when comparing it with SAN storage solutions, as there are some potential disadvantages, including:

- NAS relies heavily on network throughput, which isn't a problem when you use NAS as a file-sharing solution. However, for data-intensive apps, such as Microsoft SQL Server-based apps, NAS isn't an appropriate solution. Instead, you should consider using SAN.
- NAS provides lower throughput than SAN. This is partly because of components used and how they're connected, but also because file-level access is used.

What's a SAN?

SAN solutions are based on connectivity to a high-speed network. Components such as servers, switches, and storage devices use this high-bandwidth connection to create a high-performance storage solution. However, this high-speed connectivity comes at a cost, both monetary and in terms of required technical skills for implementation.

In a typical SAN solution, your file servers can access a storage pool that's facilitated by the SAN. The storage pool can be constructed from storage connected almost anywhere in your network.

SANs use block-level access as opposed to file-level access, so instead of having to rely on file-access protocols, such as SMB and NFS, SANs write blocks of data directly to the disks. Typically, SANs use FCo3 or iSCSI.

> **Note:** Many SANs provide flexibility by also supporting NAS-type access.

Advantages of SAN

Perhaps the most obvious advantage of SANs compared to NAS is performance. With file-level access, when a change is made to a file, even if that change is only a single data block in the file, the entire file is updated. However, with SAN, only the modified block is updated. Additionally, SANs offer several other advantages, including:

- Provision of distributed storage as a centralized pool.
- Storage that's accessible from multiple operating systems.
- Higher data throughput when it's transferred from device to device because it doesn't need to pass through a server.
- You can use SANs to build highly fault-tolerant storage solutions.

Disadvantages of SAN

There are two significant issues with using SANs. These are:

- SANs are relatively complex and often require specialist skills to deploy, provision, and maintain.
- SANs are more expensive than both DAS and NAS.

SAMPLE

> **Tip:** You can implement SANs by using several technologies, the most common of which are Fibre Channel and iSCSI. We'll discuss both in the next lesson.

Modern SAN transports

In many enterprises, Fibre Channel and iSCSI remain common SAN transports. However, modern storage platforms increasingly support NVMe over Fabrics (NVMe-oF), which is designed for very low latency and high throughput by extending NVMe semantics across a storage fabric. Windows Server 2025 includes storage enhancements that explicitly recognize NVMe-oF as part of modern SAN planning, particularly for workloads that are sensitive to latency and benefit from high IOPS density.

Comparison and scenarios for usage

It's important that you understand these storage technologies thoroughly, particularly if you're selecting your organization's storage solution. Table 1 summarizes each of these storage technologies:

Table 1: Summary of storage solutions

Storage solution	Description
DAS	Is comparatively simple with low setup costs.
NAS	Is a complementary solution for both DAS and SAN. Ubiquitous in most organizations, so well understood.
SAN	Provides the highest performance and is a feature-rich solution.

SAMPLE

When to use DAS

Based on its characteristics, you might be tempted to use DAS for single-server environments or when you want to reduce costs. Both of these are sound considerations. However, you might also consider using DAS to support departmental storage needs within a large organization, such as for a database app that's being used in a specific department. In this situation, the app management team might prefer to have local control over their storage needs. DAS is ideally suited to this need.

When to use NAS

Often the difference between NAS and SAN is somewhat obscure, largely because many SAN vendors provide file-level access and block-level access. As a result, organizations can provision

their storage using CIFS, SMB, and NFS. This means that in most large organizations, NAS shares the same storage appliances, disk shelves, and network infrastructure as SAN.

Many organizations now combine NAS-style file services on Windows Server with cloud-backed storage for cost and operational reasons. A common pattern is to keep hot data and authentication local while extending capacity and improving recovery options using Azure Files + Azure File Sync. Azure File Sync can tier colder files to the cloud while preserving a local namespace and local performance characteristics, which is especially useful for branch offices and distributed organizations.

When to use SAN

SAN provides the best storage solution for enterprise organizations, both in terms of performance and reliability. However, it's worth noting that improvements in disk technology means that for some scenarios, DAS can offer similar throughput.

Given the blurring of the lines between these storage solutions, perhaps the most compelling reason to choose SAN over any other storage solution is its expandability. Whereas DAS solutions support capacities of up to, perhaps, hundreds of terabytes (TBs), SANs can provide thousands of TBs of storage space.

To summarize, SANs offer:

- **Flexibility.** SANs provide both NAS and SAN features enabling administrators to choose for a given scenario.
- **Manageability.** SANs usually offer a unified management interface.

Table 2 provides some context of when to use which solution in a given scenario:

Table 2: When to use which storage solution

Scenario	DAS	NAS	SAN
Transactional databases requiring high performance	Low cost, but good performance. However, it might require additional administration in large enterprise organizations.	Not suitable for most database applications.	An ideal choice for transactional databases because it offers very high performance.
Virtual machine (VM) storage	Administrative overhead is higher than when using SANs but provides good performance.	A good option when trying to reduce costs and keep things simple.	Excellent performance makes this the preferred choice for this workload.

SAMPLE

Branch-office shared folders	Low cost and simple deployment make this the best choice for this workload.	Relatively simple deployment and fairly low cost. Often makes a good choice for this workload.	More expensive than other solutions, and complexity makes it a less appropriate choice.
Tiered storage for apps	Suitable for scenarios that have a limited implementation budget.	Some solutions are suitable, especially those that include Scale-Out File Server (SOFS) with Storage Spaces and tiering.	The most flexible solution for this workload. Includes features such as built-in tiering, caching, and other performance benefits.
Microsoft Exchange database and log storage	Low cost and very good performance make this a viable choice for this workload.	Not an appropriate choice.	Excellent performance makes this the preferred choice for this workload, where budget permits.

When comparing SAN to high-end direct attached storage, it's important to note that Windows Server 2025 introduces a modernized NVMe path ("native NVMe") designed to reduce overhead and improve NVMe performance on supported systems. This can make direct attached NVMe an even stronger option for certain high-performance workloads, especially when the environment can provide resiliency at the application, application, or cluster level rather than relying on a centralized SAN. Any performance-oriented storage design should be validated with representative testing before standardizing on an architecture.

SAMPLE

Block-level storage compared with file-level storage

When applications write to disks, the data is stored in files. These files comprise one or more blocks of disk space.

> **Tip:** You define block size when you format a volume on a disk.

Typically, when an application updates a file, the entire file is overwritten, and all blocks that pertain to the updated file are overwritten. This process is known as file-level storage.

For greater efficiency, it's typical when working with SANs (and some NAS appliances) to use block-level storage. In this scenario, when an application updates a file, only changed blocks are overwritten, while unchanged blocks aren't updated. When working with files that span multiple blocks in your storage, using block-level storage can significantly improve performance. Let's examine these two approaches in more detail.

File-level storage

When working with NAS, the CIFS and NFS protocols are usually implemented, although SMB is also frequently used. NAS appliances rely on file-level storage, which has the following characteristics:

- Is often less expensive than block-level storage.
- File sharing protocols (CIFS, SMB, and NFS) provide and manage access to file-level storage.
- Is implemented on block-level storage.
- Volumes using file-level storage are formatted with a file system.
- Not all applications support file-level storage, although most do.

Block-level storage

As we've learned, block-level storage is implemented in SANs. Typically, you'll use protocols such as iSCSI, Fibre Channel, or FCoE. You usually create your volumes from chunks of block-level storage. Within these volumes, you create logical unit numbers (LUNs), which are virtual storage areas. After creating the LUNs, you can make them available to your servers, which identify the LUNs as physical disks. A server administrator then creates a Windows Server volume on the "physical disk" and formats it using NTFS or ReFS.

Block-level storage has the following characteristics:

- Provides flexibility for your server administrators, enabling them to use the storage as a data volume, an OS volume, or a volume that hosts shared folders.
- Is independent of the server's OS that's accessing the storage.
- Supports file server startup, meaning you can deploy diskless servers that reply on block-level storage LUNs for the OS disks (System and Boot).
- Provides direct access from VMs to support high-performance virtualized workloads.

SAMPLE

Lesson 2: Compare Fibre Channel, iSCSI, and Fibre Channel over Ethernet

This lesson describes Fibre Channel and factors to consider when implementing it, and introduces a role service in Windows Server that enables organizations to create storage through the iSCSI protocol.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe and compare Fibre Channel, iSCSI, and FCoE.
- Describe core storage components.
- Configure iSCSI.

What is Fibre Channel?

Fibre Channel has a high-performance architecture that provides connectivity between your servers and a SAN. Fibre Channel is implemented over the Fibre Channel protocol, so in essence, it's implementing SCSI commands on a network. A Fibre Channel implementation consists of the following components:

- A SAN. This represents the storage backend and listens for computer requests.
- A computer installed with an HBA card. This is the initiator, and it initiates requests when apps require access to data that's accessible on the SAN.
- A Fibre Channel switch. Switches are used so that servers don't need a direct connection to the underlying storage on the SAN.

FCoE is a more recent implementation of Fibre Channel, and it provides excellent performance and enables you to implement Fibre Channel over your existing network infrastructure. This makes it less expensive. Using FCoE provides three advantages:

- It's easier to implement a single network technology.
- You can use most of the generic network troubleshooting tools so you don't need to learn about specific tools for storage.
- You don't usually need any specific training about the technology.

When deploying Fibre Channel, you can choose between three topologies:

- **Arbitrated loop**. Fibre Channel uses a ring to connect storage devices and requires no switches. This is seldom used these days as switches are much less expensive than they used to be.
- **Point-to-point.** Fibre Channel hosts connect directly to a storage device, negating the need for switches. Again, this is an unusual configuration nowadays as switches are inexpensive.
- **Switched fabric.** This is the most common topology. In switched fabric environments, Fibre Channel switches are used. All hosts connect to the deployed switches, and the switches connect to the backend storage.

SAMPLE

Considerations for implementing Fibre Channel

When you're planning to implement Fibre Channel, you should consider four factors carefully. These are:

- Infrastructure requirements.
- Storage-bandwidth requirements.
- Connectivity reliability and security.
- Asset and administrative costs.

Infrastructure

You'll need quite an extensive list of components to implement Fibre Channel, including:

- **Fabric or network switches.** If your network consists of fiber-optic cabling only, you'll probably use Fibre Channel switches. In networks comprising a mix of cabling types, any switches you choose must be capable of supporting different traffic types over the various media. You'll normally dedicate these switches to the Fibre Channel network. This provides performance and security benefits but does come at an increased cost.
- **HBAs.** Any hosts that must connect to the storage on the FCoE network require an HBA, either as a physical card or as a component enabled on the computer's motherboard. Each host needs at least one dedicated HBA, but ideally, you should have two to provide redundancy.
- **Cabling.** The fundamental building block of any network, including Fibre Channel. You'll need fiber optic or Ethernet cabling, or both.

  You can use Fibre Channel with several cable types, the most common of which are:
  - Single-mode fiber optic.
  - Multi-mode fiber optic.
  - Ethernet:
    - Fibre Channel over Ethernet.
    - Fibre Channel over IP.
  - Ethernet over Copper.
- **Storage controllers.** These manage the communications with backend storage.

Bandwidth

A significant benefit of using Fibre Channel is the additional bandwidth and reliability it can provide in your storage architecture. When choosing whether to implement Fibre Channel, this performance improvement can be a major factor.

Reliability and security

Fibre Channel packets are received in a specific sequence, unlike with generic TCP-based protocols and solutions. This sequencing improves throughput significantly. Additionally, you typically implement Fibre Channel deployments on a dedicated network infrastructure, so this separation from the rest of the corporate infrastructure means that security is improved because the Fibre Channel infrastructure is less susceptible to network attacks.

Costs

Fibre Channel does require personnel with specialized skills to implement it, so costs can be higher than with other storage solutions. Also, the additional infrastructure has a significant cost attached to it.

What is iSCSI?

iSCSI is a standard that defines access to storage devices by using TCP/IP protocol. Windows Server includes the iSCSI Target Server role that enables computers to access the storage

SAMPLE

connected over the network. iSCSI implementation in Windows Server has many usage scenarios, such as network and diskless boot, server-application storage, heterogeneous storage, and as an environment for development and testing.

iSCSI is a protocol that supports access to SCSI-based storage devices over a TCP/IP network. iSCSI carries standard SCSI commands over IP networks to facilitate data transfers and manage storage over a network. You can use iSCSI to transmit data on any network that works with TCP/IP protocol, including local area networks (LANs), WANs, an intranet, and the internet.

iSCSI relies on the standard Ethernet networking infrastructure, where a separate and dedicated network infrastructure is optional, and it typically connects on TCP port 3260. iSCSI protocol enables two hosts to negotiate parameters such as session establishment, flow control, and packet size, and then exchange SCSI commands by using an existing Ethernet network. By doing this, iSCSI takes a popular and high-performing local storage-bus subsystem architecture and emulates it over networks, thereby creating a SAN.

However, unlike some SAN solutions that connect to servers using special hardware, such as fiber-optic adapters and cables, iSCSI requires no specialized cabling and can be run over existing switching and IP infrastructure. You should evaluate your organization's network performance and, if needed, deploy iSCSI storage on a dedicated network.

An iSCSI deployment includes the following components:

- **IP network.** You can use standard network interface adapters and standard Ethernet protocol network switches to connect the servers to the storage device. To provide sufficient performance, the network should provide speeds of at least 1 gigabit per second (Gbps) and should provide multiple paths to the iSCSI target for high availability.
- **iSCSI targets.** iSCSI targets present or advertise storage, similar to controllers for hard-disk drives of locally attached storage. However, servers access this storage over a network, rather than locally. Many storage vendors implement hardware-level iSCSI targets as part of their storage device's hardware. Windows Server includes the iSCSI Target Server role service that you can install as a component of the File and Storage Services role, and which enables organizations to make storage available via the iSCSI protocol.
- **iSCSI initiators.** The iSCSI target displays storage to the iSCSI initiator (also known as the client). The iSCSI initiator service enables computers to connect to the iSCSI target's disk storage over the network by using the iSCSI protocol. Windows Server and client operating systems include the iSCSI initiator service.
- **iSCSI Qualified Name (IQN).** IQNs are unique identifiers that iSCSI uses to address initiators and targets on an iSCSI network. When you configure an iSCSI target, you must configure the IQN for the iSCSI initiators that'll be connecting to the target. iSCSI initiators also use IQNs to connect to the iSCSI targets. However, if name resolution on the iSCSI network is an issue, you can always identify iSCSI endpoints (both target and initiator) by their IP addresses.

iSCSI components

The main components of iSCSI protocol include the iSCSI Target Server, iSCSI initiator, and the Internet Storage Name Service (iSNS).

SAMPLE

iSCSI Target Server

The iSCSI Target Server role service provides for a software-based iSCSI disk solution. You can use the iSCSI Target Server to create both iSCSI targets and iSCSI virtual disks, and then use Server Manager to manage these iSCSI targets and virtual disks. In Windows Server, the iSCSI Target Server is available as a role service under the File and Storage Services role in Server Manager.

The features of the iSCSI Target Server in Windows Server include:

- **Challenge Handshake Authentication Protocol (CHAP).** Enable CHAP to authenticate initiator connections or enable reverse CHAP to enable the initiator to authenticate the iSCSI target.
- **Query initiator computer for ID.** Enables you to select an available Initiator ID from the list of cached IDs on the target server. It's important to note that you must use a supported version of the Windows or Windows Server systems to utilize this feature.
- **Virtual hard-disk support.** You create iSCSI virtual disks as VHDs. Windows Server supports both VHD and VHDX files, and the latter supports up to 64 TBs of capacity. You create new iSCSI virtual disks as VHDX files, but you also can import VHD files.

The maximum number of iSCSI targets per target server is 256, and the maximum number of VHDs per target server is 512, and you can manage the iSCSI Target Server by using Server Manager or Windows PowerShell.

Windows Server manages an iSCSI Target Server in hosted and private clouds by using the Storage Management Initiative Specification provider with Microsoft System Center Virtual Machine Manager.

If you want to manage iSCSI Target Server with Windows PowerShell, you can use several commands, including:

```
Install-WindowsFeature FS-iSCSITarget-Server
New-IscsiVirtualDisk E:\iSCSIVirtualHardDisk\1.vhdx –size 100GB
New-IscsiServerTarget SQLTarget –InitiatorIds "IQN: iqn.1991-
05.com.Microsoft:SQL1.contoso.com"
Add-IscsiVirtualDiskTargetMapping SQLTarget
E:\iSCSIVirtualHardDisk\1.vhdx
```

SAMPLE

iSCSI initiator

The iSCSI initiator is installed by default in all supported Windows OS versions. To connect your computer to an iSCSI target, you simply need to start the service and configure it.

The following Windows PowerShell cmdlets are examples of how you'd manage an iSCSI initiator:

- Start-Service msiscsi
- Set-Service msiscsi –StartupType "Automatic"
- New-IscsiTargetPortal –TargetPortalAddress iSCSIServer1
- Connect-IscsiTarget –NodeAddress "iqn.1991-05.com.microsoft:netboot-1-SQLTarget-target"

Considerations for implementing iSCSI

Before implementing a storage solution based on iSCSI protocol, you should carefully consider several factors, including performance, data capacity, and security, and which servers will be using the iSCSI storage and what type of physical disks you'll deploy. The main considerations during the planning process include:

- **Network speed and performance.** Network speed should be at least 1 Gbps. However, in many cases, you can deploy iSCSI networks in a datacenter with bandwidths of 10 Gbps, 40 Gbps, or even 100 Gbps.
- **High availability.** The network infrastructure must be highly available because data is sent from the servers to the iSCSI storage over network devices and components. If network components fail, data traffic must be rerouted to another network path without disrupting user experience and network performance.
- **Security.** iSCSI storage transfers data over a network, so organizations must ensure that the network is protected from different types of intrusions. In organizations where you must deploy a higher level of security, you can implement a dedicated network for iSCSI traffic, which includes iSCSI authentication.
- **Vendor information.** Read the vendor-specific recommendations to review the different types of deployments and applications that use iSCSI storage, such as Microsoft Exchange Server and Microsoft SQL Server.
- **Infrastructure staff.** IT personnel who design, configure, and administer iSCSI storage must include IT administrators with different areas of specialization, such as Windows Server, network, storage, and security administrators. This helps you design an iSCSI storage solution with optimal performance and security and create consistent procedures for management and operations.
- **Application teams.** The design team for an iSCSI storage solution should include application-specific administrators, such as Exchange Server and SQL Server administrators, so you can implement the optimal configuration for the specific technology or solution.

SAMPLE

You also should investigate competitive solutions to iSCSI and determine if they better meet your business requirements. Other alternatives to iSCSI include Fibre Channel, FCoE, and InfiniBand.

iSCSI usage scenarios

You can implement an iSCSI storage solution in multiple scenarios, depending on your organization's business requirements. The most common iSCSI usage scenarios include:

- **Network and diskless boot.** Allows organizations to deploy diskless servers by using either boot-capable network adapters or a software loader. If an application supports VHDs, organizations can save up to 90 percent of the storage space used for OS images. For example, you can use differential virtual disks in large deployments of identical OS images, such as on Hyper-V VMs or high-performance computing (HPC) clusters.
- **Server application storage.** Certain applications require block-storage use. The iSCSI Target Server can provide these applications with continuously available block storage. Because the

storage is accessible remotely, it can also combine block storage for central and branch-office locations.

- **Heterogeneous storage.** iSCSI Target Server supports iSCSI initiators that aren't based on Windows operating systems, so you can share storage on servers that are running Windows in mixed environments.
- **Lab environments.** The iSCSI Target Server role enables your Windows Server computer to be a network-accessible block-storage device, which is useful when you want to test applications prior to deploying them on SAN storage.

In addition to configuring the default (iSCSI) Target Server and iSCSI initiator settings, you can integrate these services into more advanced configurations. For example, most organizations will need to deploy high availability of the network infrastructure that connects to the iSCSI storage solution.

Demonstration: Configure an iSCSI target

For high-level demonstration steps, refer to the **Notes**, which are in the accompanying Microsoft PowerPoint presentation.

Lesson 3: Understanding iSNS, data center bridging, and MPIO

Large organizations often need advanced storage features, which can help simplify storage management. It's important you understand the components of these advanced storage features.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe iSNS, data-center bridging, and MPIO.
- Configure MPIO.

What is iSNS?

iSCSI initiator and the iSNS is a protocol used when the iSCSI initiator attempts to discover iSCSI targets. The iSNS Server service feature in Windows Server provides storage discovery and management services to a standard IP network and facilitates the integration of IP networks and manages iSCSI devices.

The iSNS server includes the following functionalities:

- Contains a repository of active iSCSI nodes.
- Contains iSCSI nodes that can be initiators, targets, or management nodes.
- Allows initiators and targets to register with the iSNS server. Initiators then query the iSNS server for the list of available targets.

SAMPLE

- Contains a dynamic database of the iSCSI nodes. The database provides the iSCSI initiators with iSCSI target discovery functionality. The database updates automatically using the Registration Period and Entity Status Inquiry features of iSNS. Registration Period allows iSNS to delete stale entries from the database. Entity Status Inquiry is similar to the ping command. It allows iSNS to determine whether registered nodes are still present on the network, and it enables iSNS to delete database entries that aren't active.
- Provides State Change Notification Service. Registered clients receive notifications when changes occur to the database in the iSNS server. Clients keep their information about the iSCSI devices available on the network up to date with these notifications.
- Provides Discovery Domain Service. You can divide iSCSI nodes into one or more groups called *discovery domains*, which provide zoning so that an iSCSI initiator can only refer, and connect, to iSCSI targets in the same discovery domain.

iSNS in modern environments

Internet Storage Name Service (iSNS) was historically used to help discover and organize iSCSI targets in larger environments by providing centralized discovery and grouping concepts. While learners may still encounter iSNS in older deployments, it is no longer a feature organizations can rely on going forward.

> **Windows Server 2025 change:** Microsoft has removed iSNS Server from Windows Server 2025. As a result, administrators should plan iSCSI discovery and management using modern alternatives rather than assuming iSNS is available as a Windows Server role/service.

SAMPLE

Recommended alternatives in modern enterprise designs:

- Use explicit target portals and well-defined discovery IP/DNS naming for iSCSI initiators (a controlled, documented configuration rather than dynamic discovery).
- Use vendor SAN management platforms for target lifecycle, zoning, and monitoring (typical in enterprise SAN operations).
- Enforce segmentation and access controls at the network and fabric layers (VLANs/subnets/zoning) and validate connectivity using standard operational runbooks.

This approach aligns with modern troubleshooting and reliability practices by reducing hidden discovery dependencies and making connectivity intentional, testable, and auditable.

What is Data Center Bridging?

Data Center Bridging is a collection of standards-based networking technologies defined by The Institute of Electrical and Electronics Engineers Inc. (IEEE) that enables support for the coexistence of LAN-based and SAN-based applications over the same networking fabric within a datacenter. Data Center Bridging uses hardware-based bandwidth allocation and priority-based flow control instead of the OS having to manage traffic itself.

Windows Server supports Data Center Bridging by installing the Data Center Bridging feature. The advantage of using Data Center Bridging is that it can run all Ethernet traffic, including traffic going to and from your Fibre Channel or iSCSI SANs. This saves on datacenter cabling, network equipment, server space, and power. Data Center Bridging is also referred to as Data Center Ethernet, Converged Enhanced Ethernet, or converged networking.

Data Center Bridging requires compatible network adapters and switches, and you can manage it using Windows PowerShell. When you install the Data Center Bridging feature, you can use the following three Windows PowerShell cmdlets: `netqos`, `dcbqos`, and `netadapter`.

What is MPIO?

Features that enable organizations to deploy redundant network connections include Multiple Connected Session (MCS) and MPIO. Although similar in the results that they achieve, these two technologies use different approaches to attain high availability for iSCSI storage connections.

MCS provides the following functionalities:

- Enables multiple TCP/IP connections from the initiator to the target for the same iSCSI session.
- Supports automatic failover. If a failure occurs, all outstanding iSCSI commands are automatically reassigned to another connection.
- Requires explicit support by iSCSI SAN devices.

MPIO provides the following functionalities:

- When multiple network interface cards and multiple network cables are installed on computers with iSCSI initiator and iSCSI target server roles, you can use MPIO to provide failover redundancy during network outages.
- MPIO requires a device-specific module (DSM) for when you want to connect to a third-party SAN device that's connected to the iSCSI initiator. The Windows OS includes a default MPIO DSM that's installed as the MPIO feature within Server Manager.
- MPIO is widely supported. Many SANs can use the default DSM without any additional software, while others require a specialized DSM from the manufacturer.
- MPIO is more complex to configure, and it isn't as fully automated during failover as MCS.

SAMPLE

MPIO best practices (2022/2025)

Multipathing improves availability only if the entire stack is consistent and validated. In enterprise practice, multipathing design should include:

- Physical and logical path separation (separate switches, NICs, and subnets where feasible)
- Consistent DSM/driver/firmware alignment per vendor guidance
- Planned failover testing under load (verify not only reconnection, but also workload behavior and performance during path loss)

Demonstration: Configure MPIO

For high-level demonstration steps, refer to the **Notes**, which are in the accompanying PowerPoint presentation.

Lesson 4: Configure sharing in Windows Server

Accessing data on the remote server over a network is a common operation in the Windows environment. To grant users access to remote resources, you must first create a share. By default, Windows computers access shares by using SMB protocol. For example, if you need to access resources on a Windows Server computer from Linux or Mac, you can install support for sharing and accessing NFS shares.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe and configure SMB and SMB shares.
- Describe and configure NFS and NFS shares.

SAMPLE

What is SMB?

If you want to access data over a network, computers must connect to the network and use a common network protocol. Most devices, including Windows Server, use TCP/IP protocol. Server Message Block (SMB) is a client/server protocol that can run on top of TCP/IP and enables you to communicate with remote computers, and then access and work with their resources, such as shares and files. SMB was developed in 1983, and Microsoft included it as part of the Network Basic Input/Output System (NetBIOS). Since then, SMB has improved, and has become more secure, especially since version 3.0, which was included in Windows Server 2012. SMB is constantly developing and improving. Windows Server 2025 supports SMB 3.1.1 and older versions of SMB protocol to version 2.0. SMB 1.0 isn't installed in Windows Server 2025 by default.

Windows uses SMB protocol for accessing resources, such as shares, files, and printers over a network on a remote computer. SMB protocol defines a series of steps, such as establishing NetBIOS session, negotiating SMB protocol dialect, and connecting to a share that must occur between the client and server before you can access the data on the remote computer. Files that are stored on the remote computer and accessed over SMB protocol for applications seem as if they are stored locally. For example, Microsoft Hyper-V can run VMs from an SMB share.

SMB protocol features

SMB protocol in Windows Server 2022 and 2025 includes the following features:

- **SMB Transparent Failover.** This feature enables you to perform the hardware or software maintenance of nodes in a clustered file server without interrupting server applications that are storing data on file shares.
- **SMB Scale-Out.** By using Cluster Shared Volumes, you can create file shares that provide simultaneous access to data files, with direct input/output (I/O), through all the nodes in a file server cluster. The **Scale-Out File Server** cluster role uses this feature.
- **Cluster Dialect Fencing.** Cluster Dialect Fencing provides support for cluster rolling upgrades for the **Scale-Out File Server** feature.
- **SMB Multichannel.** This feature enables you to aggregate network bandwidth and network fault tolerance if multiple paths are available between the SMB client and server.
- **SMB Direct.** This feature supports network adapters that have the Remote Direct Memory Access (RDMA) capability and can perform at full speed with very low data latency and by using little CPU processing time.
- **SMB Encryption.** This feature provides the end-to-end encryption of SMB data on untrusted networks and helps to protect data from eavesdropping.
- **SMB compression.** SMB protocol automatically compresses files as they're transferred over the network. Because of this, you no longer need to manually compress (zip) files to minimize network traffic and transfer files faster on slower or more congested networks.
- **Volume Shadow Copy Service (VSS) for SMB file shares.** To take advantage of VSS for SMB file shares, both the SMB client and the SMB server must support at least SMB 3.0.
- **SMB Directory Leasing.** This feature improves branch office application response times. It also reduces the number of round trips from the client to the server as metadata is retrieved from a longer-living directory cache.
- **SMB over QUIC.** SMB over QUIC (secure remote file access): SMB over QUIC provides an encrypted transport alternative to SMB over TCP, enabling access to file shares across untrusted networks without relying on a traditional VPN model. SMB over QUIC is closely associated with cloud and hybrid scenarios and is increasingly relevant for secure remote access designs.

SAMPLE

> **Note**: For Windows Server 2025, configuration is performed using PowerShell rather than Windows Admin Center.

- **Windows PowerShell commands for managing SMB.** You can manage file shares on the file server, end to end, from the command line.

SMB versions

SMB protocol is backward-compatible. Windows Server 2022 supports SMB 3.1.1 and tries to negotiate this version when communicating to a client. But if the client doesn't support SMB 3.1.1, Windows Server tries to negotiate use of an older version, to SMB 2.0. The client can be another Windows Server, a Windows 11 or even an older legacy client, or a network-attached storage (NAS) device. In Windows Server 2022, support for SMB 1.0 is disabled by default.

Table 3 lists the highest SMB version supported in Microsoft operating systems:

Table 3: Supported SMB versions

Operating system	SMB version
Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 11, and Windows 10	SMB 3.1.1
Windows Server 2012 R2, Windows 8.1	SMB 3.0.2
Windows Server 2012, Windows 8	SMB 3.0
Windows Server 2008 R2, Windows 7	SMB 2.1

SMB security hardening in Windows Server 2025

Starting with Windows Server 2025, SMB signing is required by default for both inbound and outbound SMB connections. This hardening step reduces the risk of tampering and credential relay attacks. In many environments, this change is beneficial and transparent, but it can expose legacy systems that do not support SMB signing or that rely on older access patterns. As part of an upgrade plan, administrators should validate legacy NAS devices, embedded systems, and older third-party SMB implementations for compatibility and performance.

SAMPLE

How to configure SMB shares

When you share a folder, you make its content available on the network. You can limit who can access the shared folder and share permissions. Additionally, you can limit the number of users who can access the share at the same time and specify if an offline copy of the files that users open will be created automatically on their computer.

Shared folders maintain a separate set of permissions from the file system permissions, which means that you can set share permissions even if you share a folder on the FAT file system. The same share permissions apply to all shared content. This behavior is different from file system permissions, where you can set permissions for each file individually. You can use these permissions to configure an additional level of security for files and folders that you make available on the network. You can share the same folder multiple times, by using a different share name and other share settings for each share.

In Windows Server, you can create and configure file shares with several different tools, such as File Explorer, Server Manager, Windows Admin Center, or Windows PowerShell.

> **Note:** The terms *file share* and *SMB share* refer to the same resource.

SMB share profiles

When you use Server Manager to create a new SMB share, you can select one of the following SMB share profiles:

- **Quick.** This profile doesn't have any prerequisites and asks only for basic configuration parameters when sharing a folder. After selecting the share location and share name, you can configure share settings, such as access-based enumeration, share caching, encrypted data access, and permissions.
- **Advanced.** This profile requires the **File Server Resource Manager** role service installed. It provides the same configuration options as the Quick profile, in addition to more options such as folder owners, default data classification, and quotas.
- **Applications.** This profile doesn't have any prerequisites. The profile creates SMB share with settings appropriate for Hyper-V, databases, and other server applications. Unlike the Quick and Advanced profiles, you can't configure access-based enumeration, share caching, default data classification, or quotas when you're using an Applications profile for creating a share.

Figure 1 depicts these file share profiles:

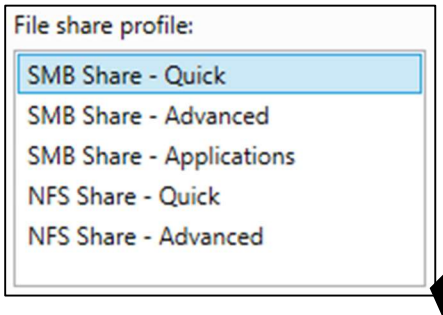

Figure 1: File share profiles in Server Manager

Table 4 lists configuration options that are available with each SMB share profile:

Table 4: SMB configuration options

Profile	Permissions	Access-based enumeration	Share caching	Encrypted data access	Data classification	Quotas
Quick	Yes	Yes	Yes	Yes	No	No
Advanced	Yes	Yes	Yes	Yes	Yes	Yes
Applications	Yes	No	No	Yes	No	No

SAMPLE

SMB share properties

As Figure 2 depicts, when you use Advanced sharing in File Explorer to create a new SMB share, you can configure the following basic properties:

- **Share name.** Each share must have a share name that's unique for Windows Server. The share name can be any string that doesn't contain special characters and is part of the Universal Naming Convention (UNC) path that Windows users use when connecting to a share. You can share the same folder multiple times and with different properties, but each share name must be unique.

> **Note:** If the share name ends with a dollar sign ($), the share is hidden and not noticeable on the network. However, you can connect to it if you know the share name and have appropriate permissions.

- **Number of simultaneous users.** This limits the number of users that can have an open connection to the share. The connection to the share is open when a user accesses the share for the first time, and it closes automatically after a period of inactivity.
- **Caching/offline settings.** You can control if the files in the share are cached and available offline on the user's computer. You can configure files to:
  - Cache on the client computer automatically when a user has network connectivity and opens them for the first time.
  - Cache offline, only if the user manually configures this and has the necessary permissions.
  - Not cache at all.
- **Permissions.** You can configure share permissions, which Windows uses in conjunction with the file system permissions when accessing data over a network. Share permissions can allow Read, Change, or Full control permissions.

SAMPLE

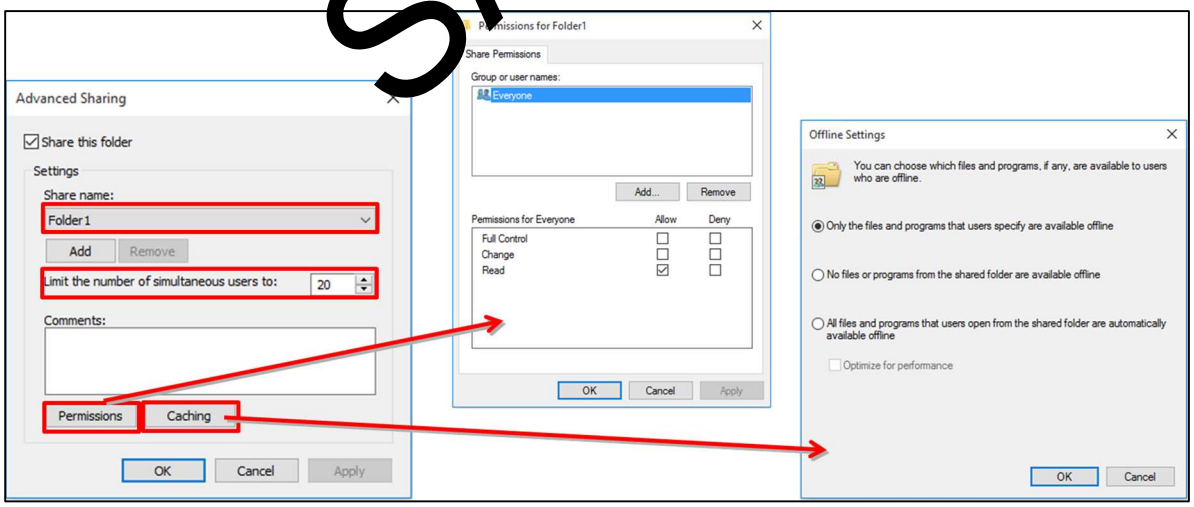

Figure 2: File share properties in File Explorer

Note: If you try to use a share name that's already in use on the computer, Windows Server provides you with an option to stop sharing an old folder and use the share name for sharing the current folder. If you rename a folder that's currently shared, you don't receive a warning. However, the folder is no longer shared.

SMB share permissions

When you share a folder, you must configure the permissions that a user or group will have when they connect to the SMB share. This is called *sharing permissions*, and there are three options:

- **Read.** Users can review content, but they can't modify or delete it.
- **Change.** Users can review, modify, delete, and create content, but they can't modify permissions. Change permission includes Read permission.
- **Full Control.** Users can perform all actions, including modifying the permissions. Full Control includes Change and Read permissions.

If you use basic sharing, by right-clicking or accessing the context menu of the folder in File Explorer and selecting the **Give access to** option, permissions are simplified and can have the following options:

- **Read.** This option allows users to observe but not modify content.
- **Read/Write.** This option is the equivalent of Full Control permissions. Users can open, modify, or delete a file, and modify permissions.

Note: Share permissions apply only to users when accessing a folder over the network. They don't apply to users who access the folder locally on the computer that stores the folder.

SAMPLE

Configure SMB shares by using PowerShell

Windows PowerShell includes the SmbShare module, which contains 44 cmdlets for managing SMB shares. This includes commonly used cmdlets, such as `New-SmbShare`, `Set-SmbShare`, and `Remove-SmbShare`. If you use the `SmbShare` cmdlets, you can configure any share properties, even those that aren't available in File Explorer and Server Manager.

The following example depicts how to create an SMB share by sharing **D:\Folder1** as a share named **Share1** by using PowerShell:

```
New-SmbShare –Name Share1 –Path D:\Folder1
```

You can review all SMB share properties for the share name **Share1** by using the following cmdlet:

```
Get-SmbShare –Name Share1 | Format-List –Property *
```

You can review the list of all cmdlets for managing SMB shares by running the following cmdlet:

```
Get-Command –Module SmbShare
```

Hybrid option: Azure Files and Azure File Sync (enterprise file services extension)

Enterprise file services often need multi-site access, cost-efficient capacity growth, or simplified recovery options. In these scenarios, Azure Files can act as a cloud-hosted SMB file share platform, and Azure File Sync can extend existing Windows Server file servers by synchronizing and optionally tiering files to the cloud while preserving a local namespace.

Recent Azure File Sync updates emphasize faster onboarding and recovery workflows, improved performance for large sync operations, and explicit support for Windows Server 2025 deployments. When designing hybrid file services, treat Azure File Sync as an extension strategy—not a replacement for sound on-prem file server design: continue to apply correct SMB security settings, permissions hygiene, and monitoring for both local and cloud components.

Demonstration: Configure SMB shares by using Server Manager and Windows PowerShell

For high-level demonstration steps, refer to the Notes, which are in the accompanying PowerPoint presentation.

What is NFS?

Windows Server uses SMB protocol for sharing and accessing shared resources by default. But SMB isn't the only protocol that provides access to network resources. NFS is a distributed file system protocol that provides similar functionality, mostly used by UNIX systems. It's based on open standards and allows access to a file system over a network. NFS was introduced by Sun Microsystems in 1984 and has been developing actively since then—its current version is 4.2 (August 2022).

> **Note:** NFS provides access to exports. Exports are similar to SMB shares in Windows; they are shared UNIX file system paths.

Windows Server doesn't include support for NFS by default. If you want to use the NFS protocol for transferring files between Windows and non-Windows systems, such as Linux or UNIX, you need to install support for NFS in Windows Server. As Figure 3 depicts, the two components for NFS support in Windows are:

- **Client for NFS.** This feature enables a Windows Server to access NFS exports on an NFS server, regardless of the OS on which NFS server is running. **Client for NFS** supports NFSv2 and NFSv3.

SAMPLE

- **Server for NFS.** This role service enables a Window Server to share folders and make them available over NFS. Any compatible NFS client can access the shares, regardless of the OS on which the NFS client is running. **Server for NFS** supports NFSv2, NFSv3, and NFSv4.1.

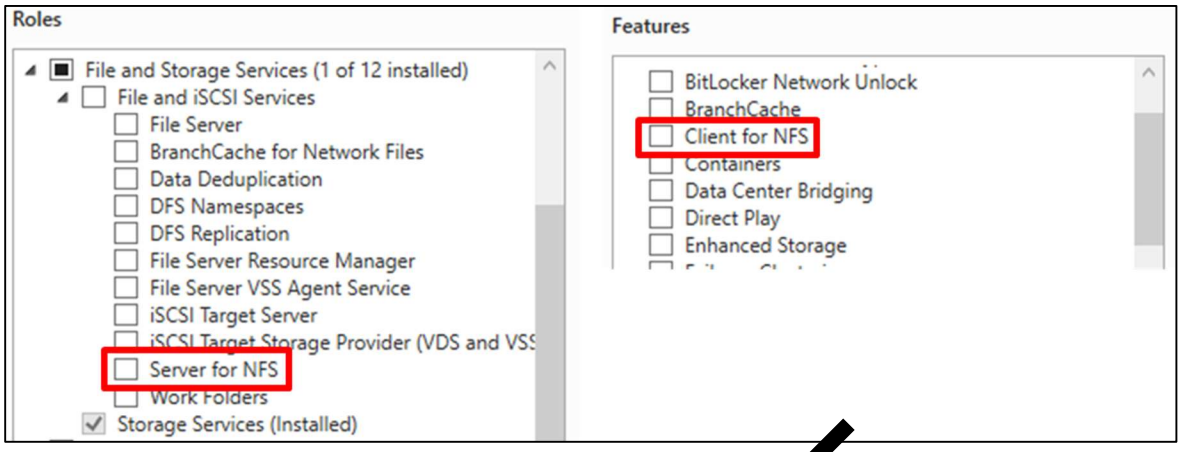

Figure 3: Adding the **Server for NFS** role service and **Client for NFS** feature in Server Manager

NFS components in Windows Server have been improved and expanded in every Windows Server version. **Server for NFS** includes support for Kerberos protocol version 5 (v5) authentication. Kerberos protocol v5 authentication provides authentication before granting access to data. It also uses checksums to prevent data tampering. **Server for NFS** supports NFS version 4.1, which includes improved performance with the default configuration, native Windows PowerShell support, and faster failovers in clustered deployments.

SAMPLE

NFS sharing usage scenarios

You can use NFS in Windows Server in many scenarios. Common scenarios include:

- **VMware VM storage.** In this scenario, VMware hosts VMs on NFS exports. You can use **Server for NFS** to host the data on a Windows Server computer.
- **Multiple OS environments.** In this scenario, your company uses a variety of operating systems, including Windows, Linux, and Mac. The Windows file-server system can use **Server for NFS** and the built-in Windows sharing capabilities to ensure that all the operating systems can access shared data.
- **Merge or acquisition.** In this scenario, two companies are merging. Each company has a different file server infrastructure. Users in one company use NFS, while the other uses SMB to access shared data. By implementing **Client for NFS** and **Server for NFS**, users can access data on file servers in both companies.

How to configure NFS shares

Before you can create an NFS share on Windows Server, you must install the **Server for NFS** role service. After you install the role service, you can use Server Manager or PowerShell to create the NFS share. With Server Manager, you can create NFS shares similarly to creating SMB shares by using NFS Share - Quick or NFS Share – Advanced profiles. While the Quick profile doesn't have

additional prerequisites, the Advanced profile requires the **File Server Resource Manager** role service to be installed.

Windows PowerShell includes the NFS module, which contains 42 cmdlets for managing NFS shares. This includes cmdlets such as `New-NfsShare`, `Set-NfsShare`, and `Remove-NfShare`. You can review a list of all cmdlets for managing NFS shares by running the following cmdlet:

```
Get-Command –Module NFS
```

Demonstration: Configure an NFS share by using Server Manager

For high-level demonstration steps, refer to the **Notes**, which are in the accompanying PowerPoint presentation.

Lab 3: Plan and configure storage technologies and components

Lab 4: Configure SMB over QUIC

Please refer to our online labs to supplement your learning experience with exercises.

Knowledge check

Check your knowledge by answering these questions:

1. Name the client and the server component of the iSCSI protocol.
2. Name two usage scenarios for iSCSI storage.
3. Which Windows Server role service is required to enable you to create SMB shares with the advanced profile?
4. What must you install if you want to create NFS share on Windows Server?

> **Note:** To find the answers, refer to the **Knowledge check** slides in the accompanying PowerPoint presentation.

SAMPLE