Project Title : Centralized Data Storage & Backup with DFS and Windows Server Backup.

Microsoft Certified Solutions Associate

Author: Bhavesh Mayekar
Course: Microsoft Certified Solutions Associate
Date: 2025-09-08 (linkedin.com/in/bhaveshmayekar)

Objectives

The goal of this project is to design and implement a resilient file service where users access a single, consistent namespace, with automatic replication across servers for high availability, and with daily backup policies for disaster recovery.

Key technologies used:

- DFS Namespace (DFSN): Provides a unified folder path for users (e.g., \\domain.local\Company).
- DFS Replication (DFSR): Ensures data consistency between multiple file servers.
- Windows Server Backup (WSB): Protects data by creating scheduled and on-demand backups.

Why This Project Matters (Concepts Explained Simply)

- Centralized Data Access: Users don't need to remember multiple server paths; one namespace works everywhere.
- High Availability with DFSR: If one server goes down, the other server still provides access-zero downtime for file services.
- Data Protection with Backup: Even if data is deleted/corrupted, administrators can restore it from backup.
- Best Practice: Combines redundancy (replication) with disaster recovery (backup) to meet enterprise IT standards.

Executive Summary

This project demonstrates how to build a resilient, highly-available file service using DFS Namespace and DFS Replication (DFSR), combined with scheduled backups using Windows Server Backup. The solution provides a single, friendly UNC path for users while ensuring data redundancy, faster recovery, and automated daily backups to reduce data loss and operational risk

Skills & Technologies Demonstrated

Windows Server (2016/2019/2022+), Active Directory, DFS Namespaces, DFS Replication (DFSR), Windows Server Backup (WSB/wbadmin)SMB, NTFS permissions, Event Viewer, backup & restore best-practices.

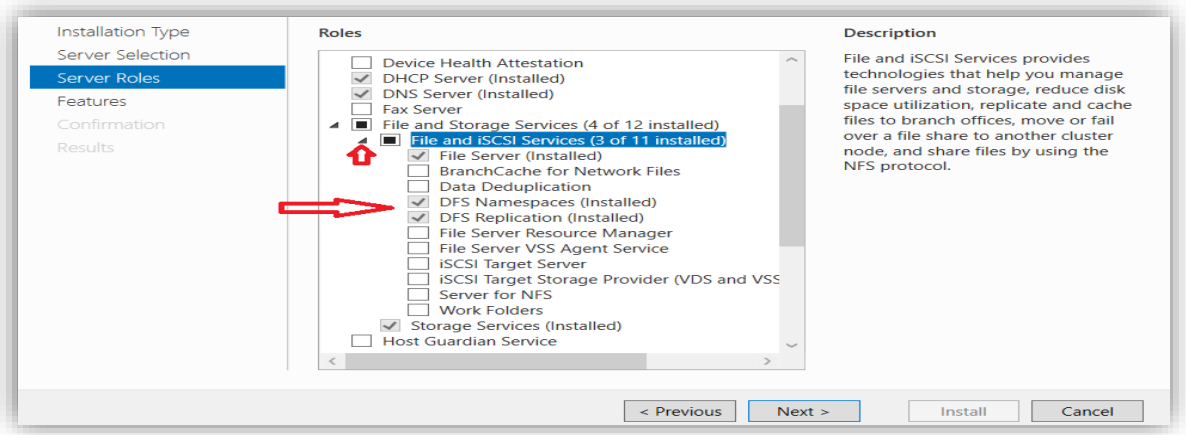
Lab Environment Setup

- Server 1: Domain Controller with AD DS (Domain:Microsoft.com)
- Server 2: Member Server (File Server role)
- Client 1: Windows 10/11 client joined to domain

Step-by-step Implementation

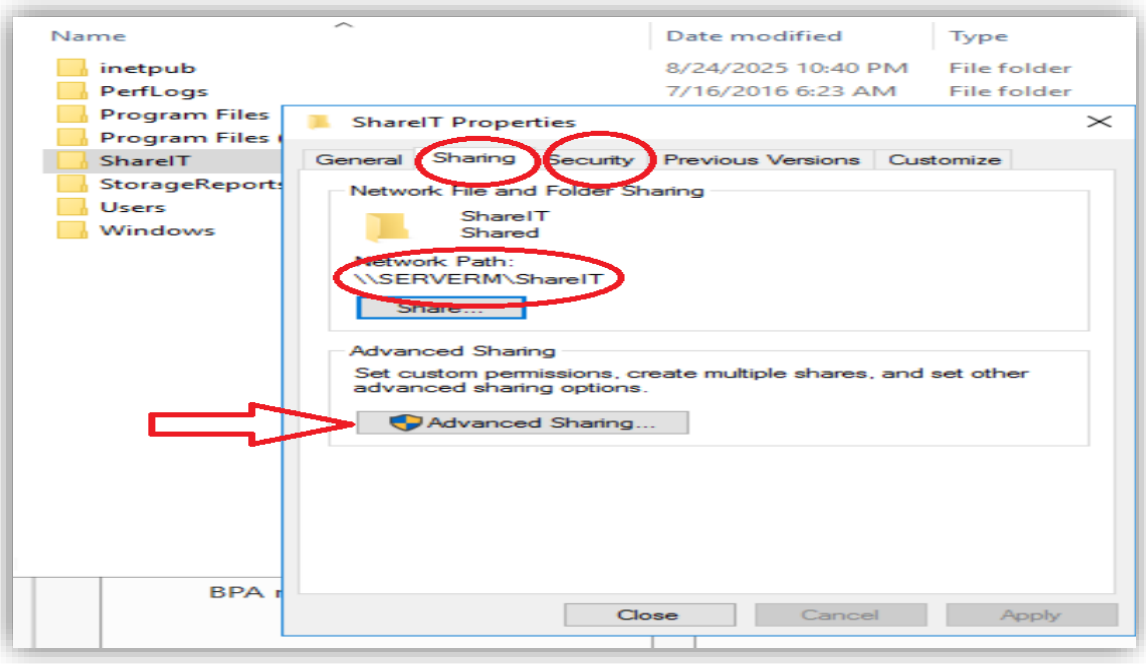
Step 1 – Install DFS Roles

1. On both Server 1 (DC) and Server 2 (MS)
    - Open Server Manager → Manage → Add Roles and Features.
    - Select Role-based installation.
    - Check File and Storage Services → File and iSCSI Services → DFS Namespaces and DFS Replication.
    - Click Next → Complete installation and restart if required.



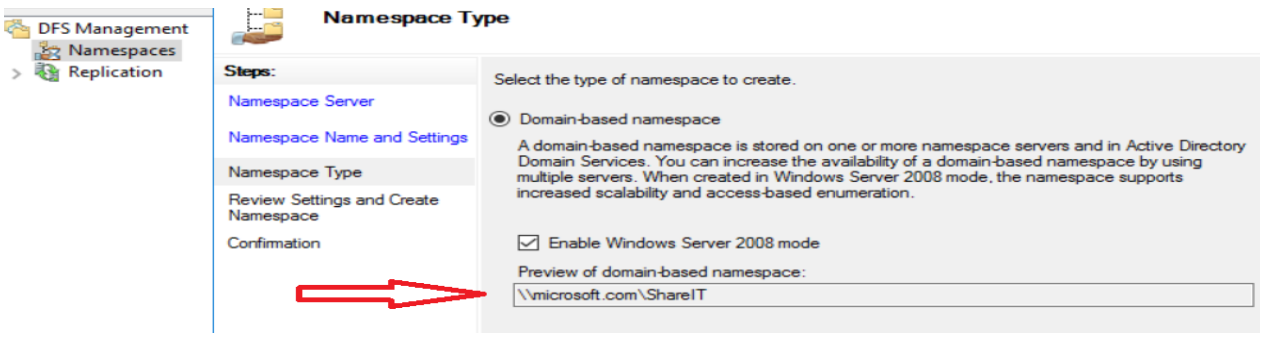
Step 2 – Create Shared Folder on Server 2 and Client 1

1. Create folder: D:\ShareIT.
2. Right-click folder → Properties → Sharing → Advanced Sharing → Share this folder.
    - Share Name: ShareIT
    - Permissions: Add group Domain Users → Read/Change.
    - Add Domain Admins → Full Control.
3. NTFS Permissions (Security tab): Same as above (least privilege).



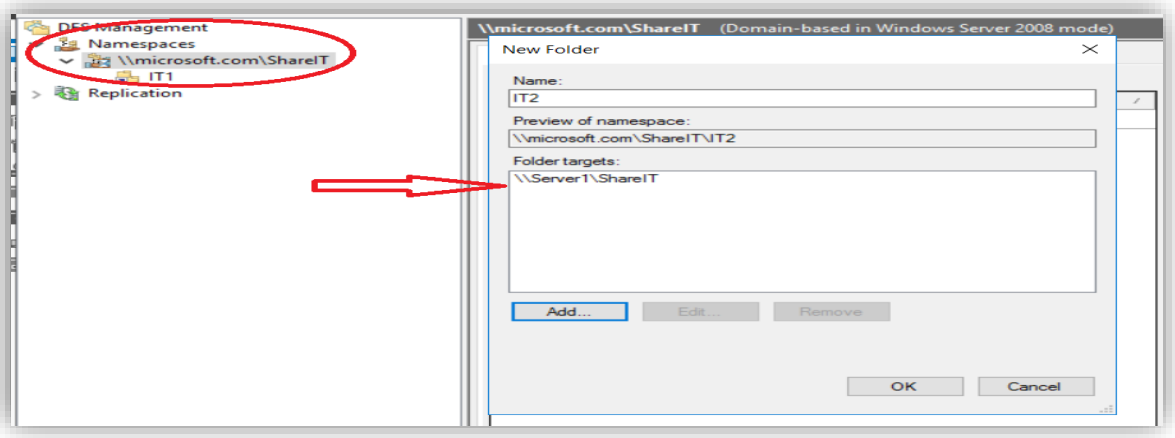
Step 3 – Create DFS Namespace

1. On Server 1 (DC1): Open DFS Management on Win+R (dfsmgmt.msc).
2. OR tools → DFS management
3. Right-click Namespaces → New Namespace.
4. Select Server 1 as the host server.
5. Namespace Name → Company.
   UNC Path will be ex : \\microsoft.com\ShareIT
6. Choose Domain-based namespace (Windows Server 2008 mode).
7. Finish wizard.



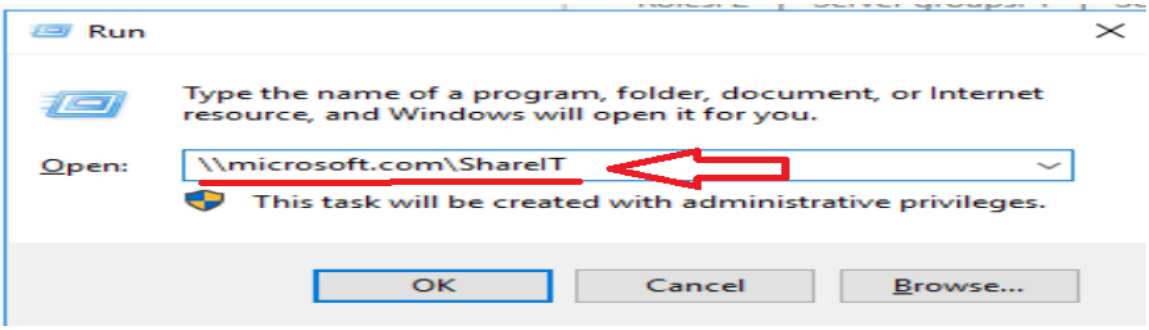
Step 4 – Add Folder to Namespace

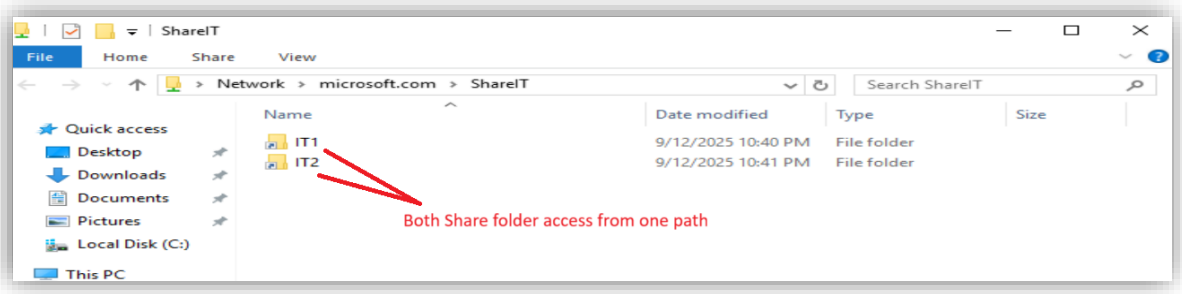
1. In DFS Management, expand \\microsoft.com \ShareIT
2. Right-click → New Folder → Name: ShareIT.
3. Add Folder Target → \\Server2\ShareIT.
4. Confirm it appears under \\microsoft.com\ShareIT



Step 5 – Verify Access from Client

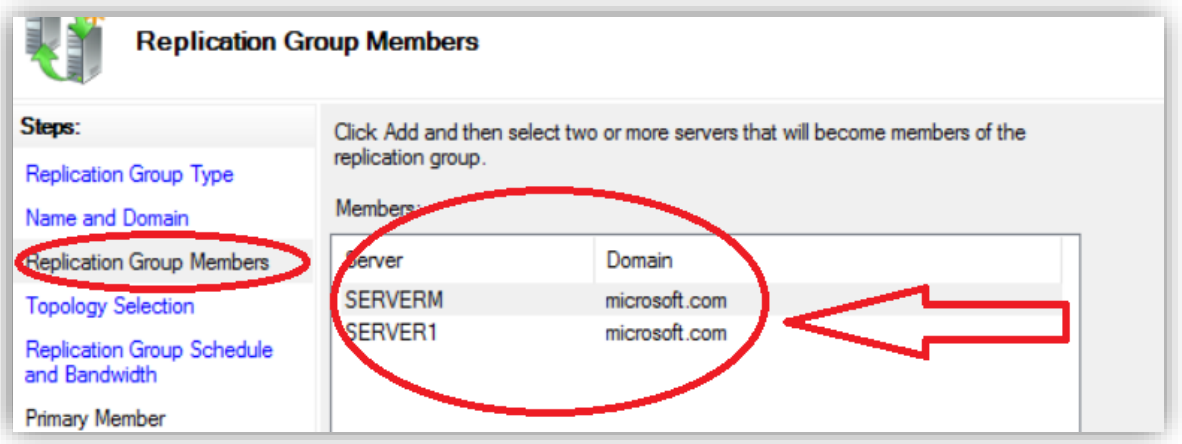
1. On Client01 (domain-joined):
    - Open Run → \\microsoft.com\ShareIT
    - Create a test file → check if accessible.

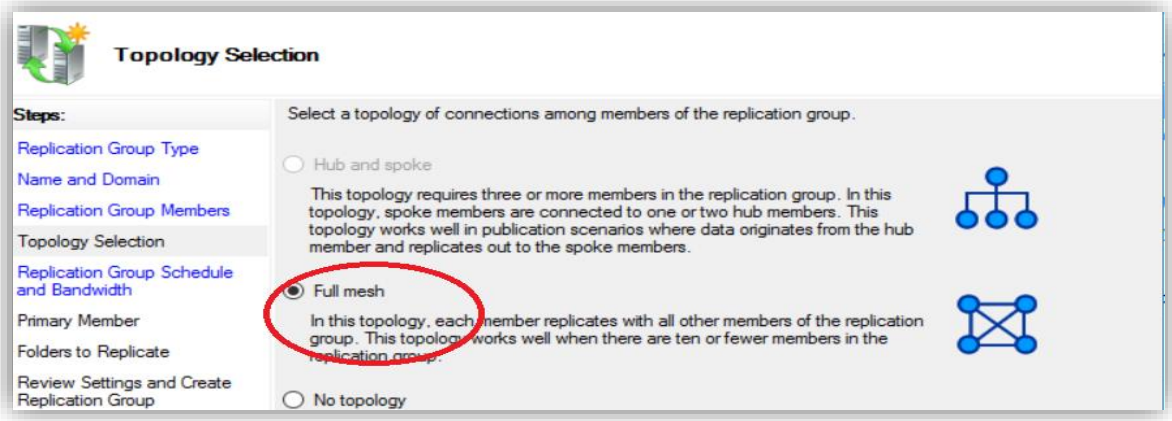


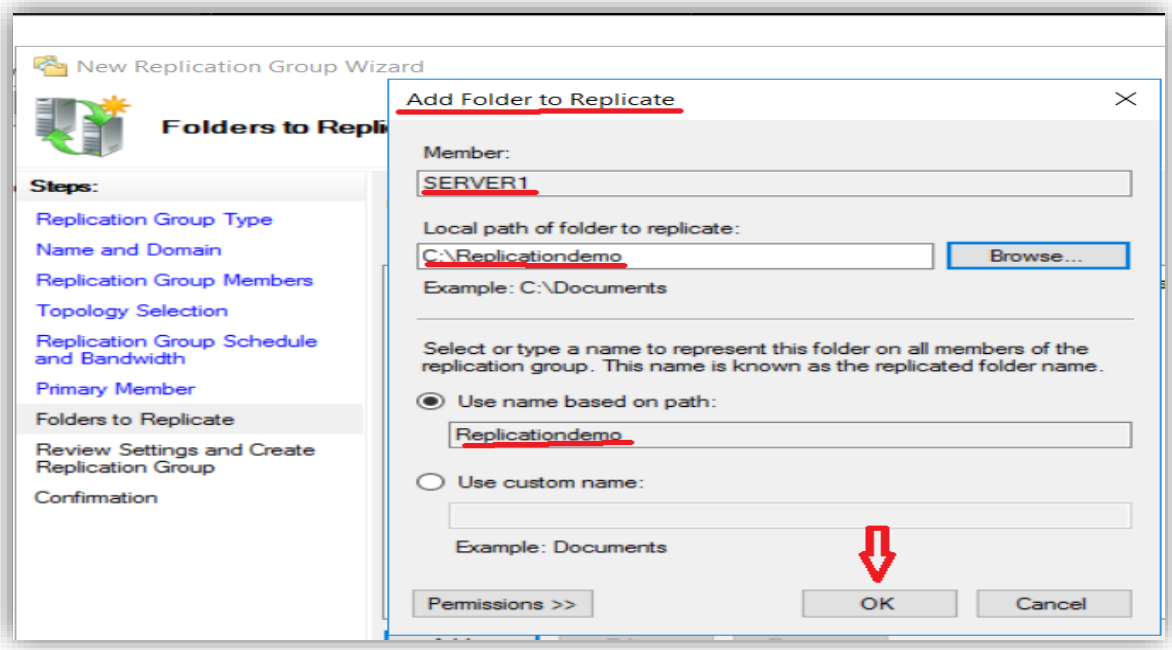


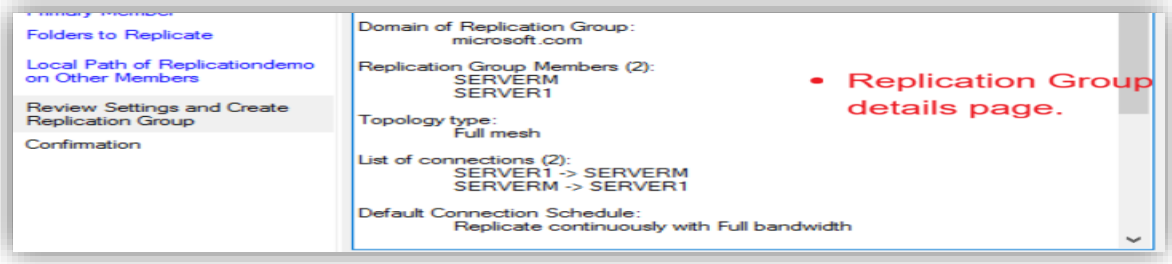
Step 6 – Configure DFS Replication

1. In DFS Management → Right-click Share folder → **Add Folder Target** → \\server2\ShareIT
2. Wizard asks to create **Replication Group**. Select:
    - **Topology:** Full Mesh.
    - **Replication Schedule:** Full (24/7).
    - Set **Primary Member** (SERVER 1).
3. Finish wizard.



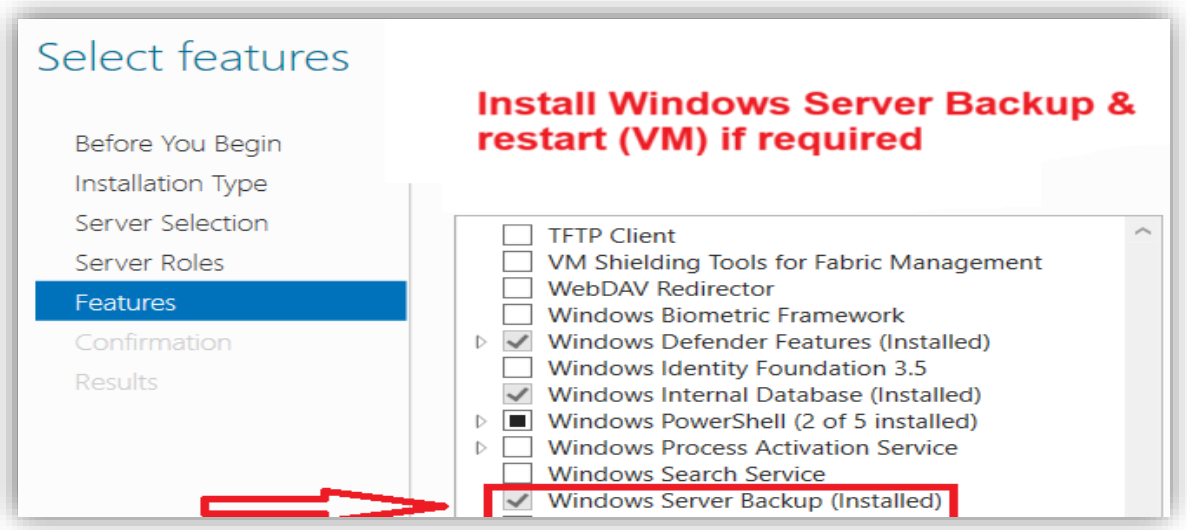

Topology Selection
Steps:
Replication Group Type
Name and Domain
Replication Group Members
Topology Selection
Replication Group Schedule and Bandwidth
Primary Member
Folders to Replicate
Review Settings and Create Replication Group
Select a topology of connections among members of the replication group.
Hub and spoke
This topology requires three or more members in the replication group. In this topology, spoke members are connected to one or two hub members. This topology works well in publication scenarios where data originates from the hub member and replicates out to the spoke members.
Full mesh
In this topology, each member replicates with all other members of the replication group. This topology works well when there are ten or fewer members in the replication group.
No topology


New Replication Group Wizard
Folders to Repli
Steps:
Replication Group Type
Name and Domain
Replication Group Members
Topology Selection
Replication Group Schedule and Bandwidth
Primary Member
Folders to Replicate
Review Settings and Create Replication Group
Confirmation
Add Folder to Replicate
Member:
SERVER1
Local path of folder to replicate:
C:\Replicationdemo
Browse...
Example: C:\Documents
Select or type a name to represent this folder on all members of the replication group. This name is known as the replicated folder name.
Use name based on path:
Replicationdemo
Use custom name:
Example: Documents
Permissions >>
OK
Cancel


Folders to Replicate
Local Path of Replicationdemo on Other Members
Review Settings and Create Replication Group
Confirmation
Domain of Replication Group:
microsoft.com
Replication Group Members (2):
SERVERM
SERVER1
Topology type:
Full mesh
List of connections (2):
SERVER1 -> SERVERM
SERVERM -> SERVER1
Default Connection Schedule:
Replicate continuously with Full bandwidth
Replication Group details page.

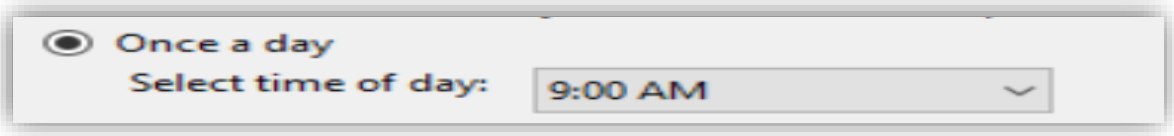
Step 7 – Install Windows Server Backup

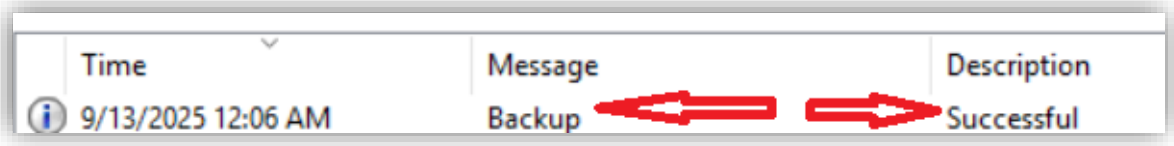
1. On Server 1: Open Server Manager → Add Roles and Features → Features.
2. Check Windows Server Backup.
3. Install

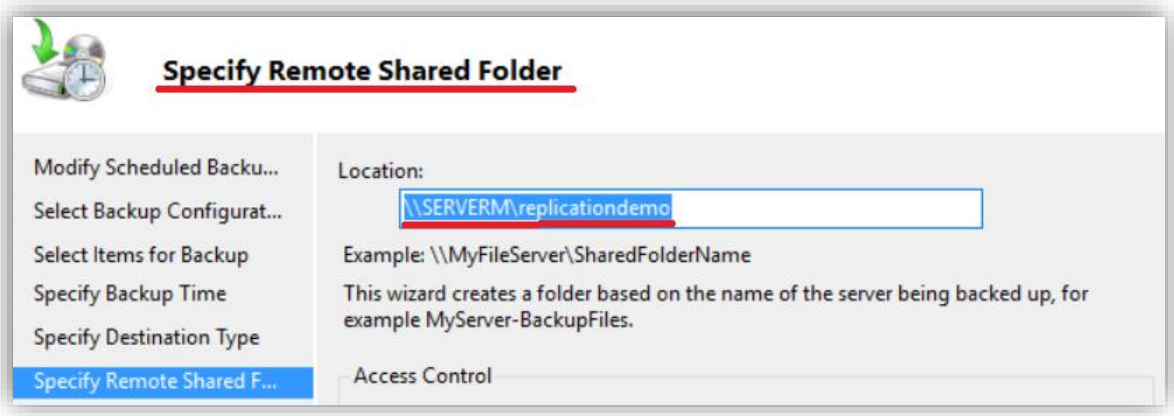


Step 8 – Configure Backup Schedule

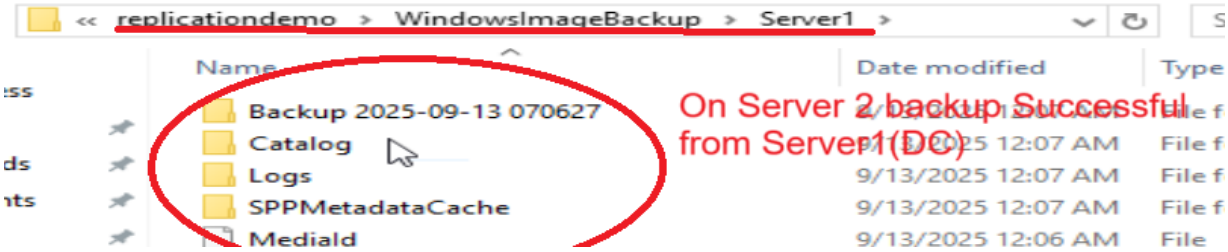
1. Open Windows Server Backup (wbadmin.msc). o
2. In right panel → Backup Schedule wizard.
3. Select Full Server (recommended) or Custom → D:\DeptShare.
4. Choose Backup to dedicated hard disk or Network Share Path.
5. Set Daily Schedule (e.g., 9 AM).
6. Finish.







- **Verify Access If two servers are present: Windows Server Backup**
  - **Shut down server 1 → access still works from server 2**



Troubleshooting :

- DFS not working → Check namespace path, DNS resolution, and AD replication.
- Backup fails → Ensure enough space and correct permissions on backup target.
- Slow replication → Verify schedule (default 24/7) and staging folder size.
- If Scheduled backup take time do backup once

Conclusion:

I successfully completed the project **"Centralized Data Storage & Backup with DFS and Windows Server Backup."**
Through this implementation, I was able to:

- Create a **centralized namespace** so users access data through a single, simple path.
- Configure **DFS Replication** to ensure data is always available across multiple servers.
- Set up **daily backup schedules** to protect data from accidental loss or corruption.

This project reflects how IT teams in real organizations combine **high availability** with **disaster recovery** to keep business operations running smoothly. It gave me a deeper understanding of **enterprise storage solutions, data protection, and best practices** used in production environments.

Author: Bhavesh Mayekar
Course: Microsoft Certified Solutions Associate
Date: 2025-09-08 (linkedin.com/in/bhaveshmayekar)