A comprehensive, step-by-step guide to resolve this SYSVOL replication failure

Problem Statement: SYSVOL Replication Failure and Missing Shared Folders

Environment:

Domain: VNKN01.local (Windows Server 2019)

Domain Controllers:

VNKN01-ADS-01 (PDC Emulator): 192.168.62.11 (Autorotative DC)

VNKN01-ADS-02 (DC): 192.168.62.12 (non-Autorotative DC)

VNKN01-ADS-03 (DC): 192.168.62.15 (non-Autorotative DC)

Prerequisites* for All DCs:** You must first install the AD DS role and then run the promotion wizard for the SYSVOL folder to be created on the local drive. This *folder, located at* ***C:\Windows\SYSVOL

Symptom: *The SYSVOL and NETLOGON shared folders are present and accessible on VNKN01-ADS-01 but are missing on VNKN01-ADS-02 and VNKN01-ADS-03. The local C:\Windows\SYSVOL directory exists on all DCs.*

Observation: *Active Directory replication for objects (users, GPOs) functions correctly across all domain controllers.*

Hypothesis: *The issue is a failure in Distributed File System (DFS) Replication for the SYSVOL share, while core AD replication is healthy.*

Analysis The Environment:

Event ID 4012 was found on all domain controllers, indicating that DFSR (Distributed File System Replication) has stopped.
To restore SYSVOL replication, Authoritative Synchronization must be performed.
The DC with the latest and most complete policy folders (in this case, VNKN01-ADS-01) will act as the Authoritative Synchronization Source.

Purpose

Phase 0 – *When and Why to Use Non-Authoritative Synchronization in Your Scenario*
Phase 1 – *To resynchronize SYSVOL among DCs when replication halts (e.g., Event ID 4012).*
Phase 2 – *Rebuilding Missing SYSVOL / NETLOGON Shares in a DFSR Environment*

Basic concept of Replication: Active Directory & SYSVOL Replication

🔁 Replication in Active Directory

When a server is promoted to a **Domain Controller (DC)** in Active Directory, two key components are automatically set up and **replicated across all Domain Controllers** in the domain **(NTDS and SYSVOL)**:

🗃️ 1. Active Directory Database Replication (AD Replication)

- **Database Involved:** ntds.dit (the core AD database)
- **What it Contains:** Users, groups, computers, OUs, group memberships, etc.
- **Purpose:** Ensures that all changes (e.g., creating a new user) are synced across all Domain Controllers.
- **Replication Protocol:**
  🔧 **RPC (Remote Procedure Call)** over IP
  - Efficient, secure, and handles replication between sites as well.

📁 2. SYSVOL Folder Replication

- **What is SYSVOL?**
  A shared folder on all Domain Controllers that stores:
  - **Group Policy Objects (GPOs)**
  - **Logon/logoff scripts**
  - Other public domain-wide scripts or files
- **Purpose:** Ensures all DCs have the same policies and scripts for consistent application to users and computers.
- **Replication Protocol:**
  🔄 **DFSR (Distributed File System Replication)** *(modern and default in newer Windows Server versions)*
  - Replaces the older **FRS (File Replication Service)**
  - More reliable and efficient for file replication

🔑 Key Points:

- **Replication is automatic** once a server is a Domain Controller.
- Ensures **high availability and consistency** across the domain.
- **AD Database** → Replicated via **RPC**
- **SYSVOL Folder** → Replicated via **DFSR**

To summarize our discussion, there are two categories of replication: the first is **AD replication**, and the second is **SYSVOL replication**. The AD replication is responsible to relicate the AD database (**NTDS.dtl**) i.e. replicate user and computer information, including account details for every user, computer, group, and other entities within the entire domain or forest. Conversely, SYSVOL replication replicate the **policy** and **script** directories across our domain, ensuring these folders are accessible on all client machines and domain controllers.

*Before tackling problems related to SYSVOL Replication, it's crucial to keep in mind the differences between **authoritative** and **non-authoritative** synchronization among domain controllers.*

- Authoritative sync means the source domain controller is **treated as the master**, and its policies or SYSVOL data are pushed to all other domain controllers. Other controllers overwrite their data with that from the authoritative source.
- Non-authoritative sync means the target domain controller copies the policies or data from another domain controller (usually the primary or source controller) to update itself.
- If the primary domain controller has updated Sysvol information, initiate synchronization from it to the additional domain controllers. If the additional domain controllers also have updated Sysvol information, then initiate a sync from the additional domain controllers back to the primary domain controller.

All DCs are aligned well with best practices for ensuring policy replication and consistency across domain controllers.

SYSVOL Sync: Authoritative vs. Non-Authoritative

- **Authoritative Sync (D2)**: Restores SYSVOL for the entire domain from a single, correct DC. Replicates **FROM** that DC.
- **Non-Authoritative Sync (D4)**: Repairs a single, broken DC by pulling data from a healthy DC. Replicates **TO** that DC.

SYSVOL local and SYSVOL share are two terms

Every Domain Controller (DC) maintains a critical folder known as **SYSVOL**. This local folder holds essential domain files, most importantly **Group Policy Objects (GPOs)** and logon scripts.

To make these policies available to clients, the local folder is exposed over the network as the `\\DomainName\SYSVOL` e.g. \\VNKN01.local\SYSVOL shared resource.

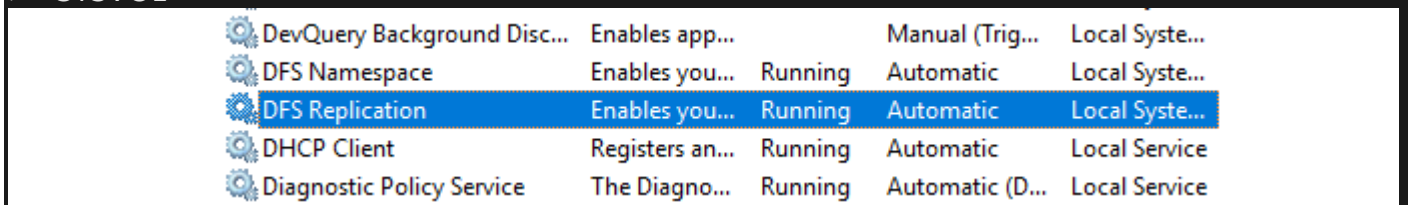
Synchronization across the entire domain is handled by the **DFS Replication** (DFSR) service. Any policy changes made, typically originating on the **PDC Emulator** (the authoritative DC), are swiftly replicated by DFSR to the local SYSVOL folder of every other DC.

This process ensures that all SYSVOL shares are always consistent, guaranteeing that users and computers receive the correct, up-to-date policies from any DC they connect to.

The term SYSVOL refers to a set of files and folders that reside on the local hard disk of each domain controller in a domain and that are replicated by the File Replication service (DFRS Replication). Network clients access the contents of the SYSVOL tree by using the following shared folders:

- NETLOGON

- SYSVOL



- https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/missing-sysvol-and-netlogon-shares

DNS Testing

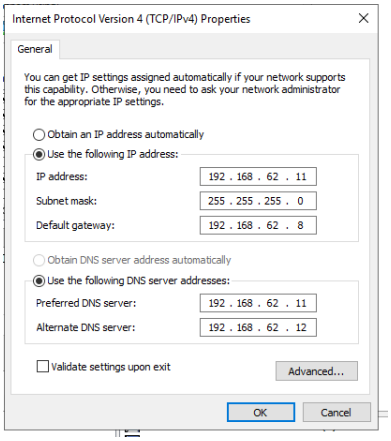
Step 1: *Verify DNS Server Settings*

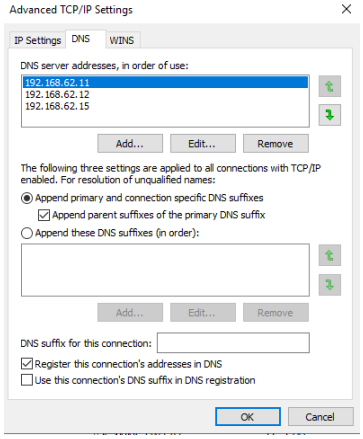
I. Check if the DNS service (port 53) is open on the server

```
Test-NetConnection -ComputerName 192.168.0.11 -Port 53
```

II. VNKN01-ADS-01 (PDC Emulator):

Its primary DNS should be its own loopback address or its static IP address (127.0.0.0.1 or 192.168.62.11). It should also have the other DCs' IP addresses (192.168.62.12, 192.168.62.15) as secondary DNS servers.

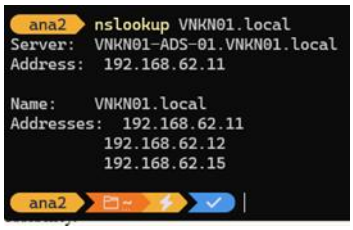


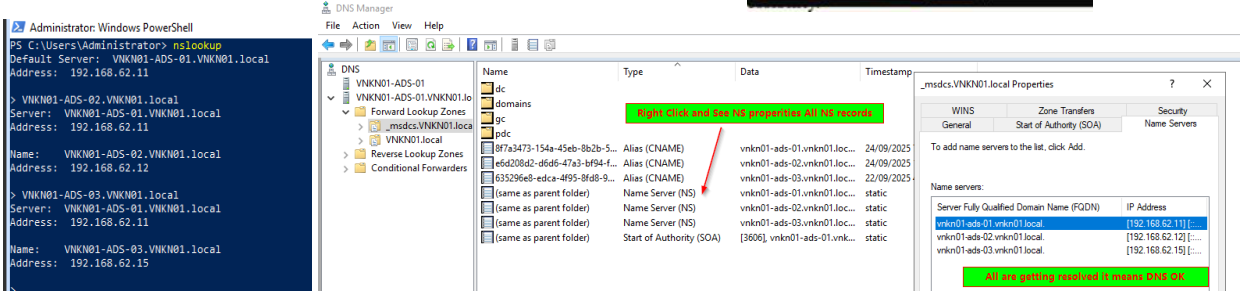


Step 2*: Manual DNS Resolution and Record Verification*

- *Internal Name Resolution (NS) Test*

Run on VNKN01-ADS-01:
nslookup VNKN01-ADS-02.VNKN01.local
nslookup VNKN01-ADS-03.VNKN01.local

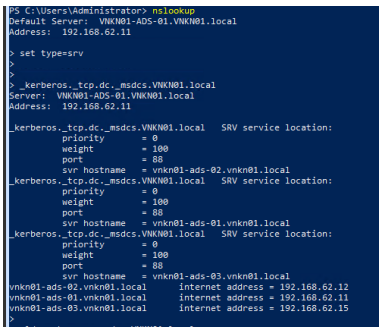


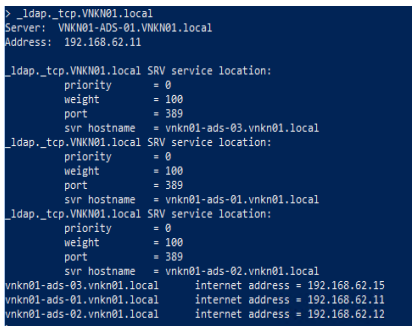


All is resoved so it is ok

❖ *Service Locator (SRV) Record Test (It allows clients to find domain)*

nslookup
set type=SRV
_kerberos._tcp.dc._msdcs.VNKN01.local
_ldap._tcp.gc._msdcs.VNKN01.local
_ldap._tcp.VNKN01.local
exit



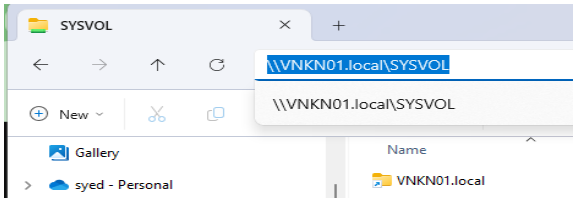


Show that Kerberos, Global Catalog (GC) and Domain Controller-specific Services is OK

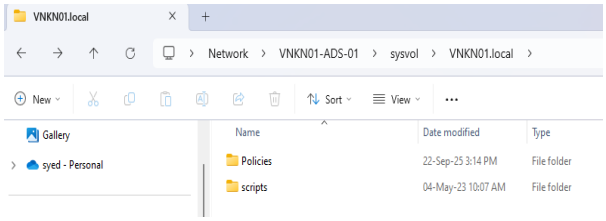
If you check the SYSVOL share is **working good** on your domain **VNKN01.local.** Here are some methods we can use from **any domain client**:

Method 1: Using Windows Explorer Address Bar

Type one of these paths in the address bar of Windows Explorer**:\\VNKN01.local\SYSVOL** having both subfolder **polices** and **scripts.**

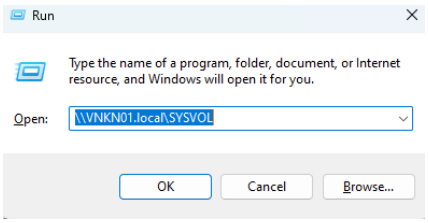


OR



Method 2: Using Run Dialog

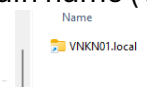
1. Press Windows + R
2. Type: \\VNKN01.local\SYSVOL
3. Press Enter



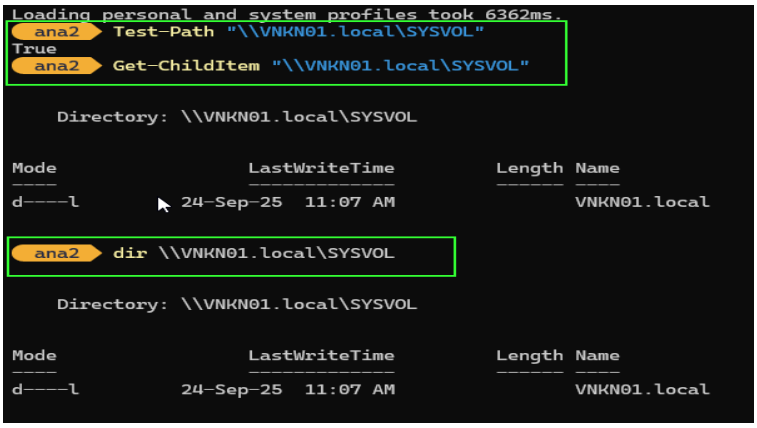
What You Should See:

If SYSVOL is working correctly, you should see:

- A folder (shortcut folder) containing your domain name (VNKN01.local)
- Subfolders like "Policies" and "scripts"
- Group Policy objects and logon scripts



Method 3: Command Prompt or PowerShell Check to run any client.



If shurtcut(VNKN01.local) folder is missing (SYSVOL BROKEN) *the Troubleshooting*

So, note 😢) In over Case SYSVOL replication is broken down or missing.

*(Missing Netlogon and SYSVOL folder by check by using **net share** cmd)*

🧩 Step-by-Step Recovery Guide

Step 1 – Verify the DFSR and Netlogon Services

Check if both DFS Replication and Netlogon services are running:

```
Get-Service -Name DFSR, Netlogon | Select-Object Name, Status, StartType
```

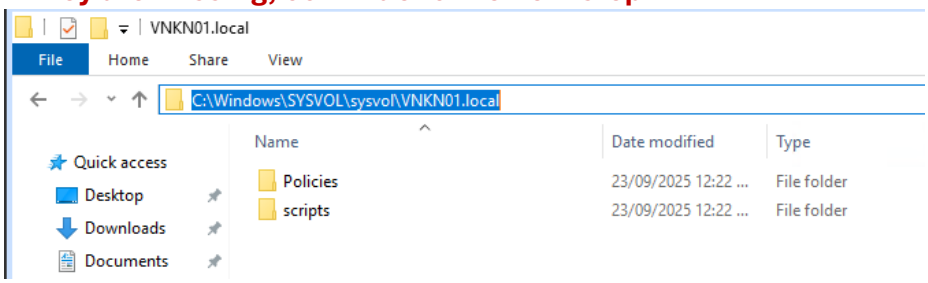
If either service is stopped, restart it:

```
Start-Service -Name DFSR, Netlogon
```

Step 2 – Check if SYSVOL and NETLOGON Shares Exist

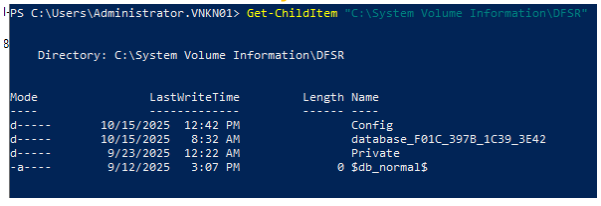
```
Get-SmbShare -Name SYSVOL, NETLOGON
```

If they are missing, continue to the next step.



If it's missing or empty, confirm the local DFSR data folder exists:

```
Get-ChildItem "C:\System Volume Information\DFSR"
```



If the folder is empty or missing, your replication may have broken — proceed with Authoritative Synchronization (Phase 1 steps).

Phase 0 – When and Why to Use Non-Authoritative Synchronization in Your Scenario

What "Non-Authoritative Synchronization" Means

In DFSR, **Non-Authoritative Synchronization** is used when a **particular domain controller** has **stale, incomplete, or outdated SYSVOL data**, but other DCs still have correct copies.

Instead of overwriting the "good" data from others, you tell DFSR:

"Hey, this DC's copy is bad — throw it away and resync everything fresh from the authoritative one."

In short:

- **Non-Authoritative Sync** → One DC pulls data from others.
- **Authoritative Sync** → One DC pushes data to all others.

Situation	Explanation
🧩 **One DC's SYSVOL folder is incomplete, empty, or outdated**	Example: `VNKN01-ADS-03` has missing or old Group Policy Objects, while `VNKN01-ADS-01` and `VNKN01-ADS-02` are fine.
⚠️ **Replication broken on one DC only (Event ID 4012 on a single DC)**	Indicates that DC fell out of sync — Non-Authoritative Sync will make it download a new copy.
🔄 **After restoring a domain controller from backup or snapshot**	If a DC was recovered from backup, its SYSVOL contents may be older. You must mark it non-authoritative, so it resyncs from a healthy DC.
📀 **You performed Authoritative Sync on one DC**	After performing **Authoritative Sync** on `VNKN01-ADS-01`, the other DCs (`VNKN01-ADS-02` and `VNKN01-ADS-03`) automatically perform **Non-Authoritative Sync** to pull the updated data.

Example: Fixing only VNKN01-ADS-03 (bad SYSVOL)

1. **Stop DFS Replication Service**
   ```
   Stop-Service DFSR
   ```
2. **Disable DFS Replication for SYSVOL**
   ```
   Set-ADObject -Identity "CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=VNKN01-ADS-03,OU=Domain Controllers,DC=VNKN01,DC=local" `
   -Replace @{msDFSR-Enabled=$false}
   ```
3. **Wait for Event ID 4114** (replication disabled confirmation).
4. **Re-enable DFS Replication**
   ```
   Set-ADObject -Identity "CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=VNKN01-ADS-03,OU=Domain Controllers,DC=VNKN01,DC=local" `
   -Replace @{msDFSR-Enabled=$true}
   ```
5. **Start DFSR Service**
   ```
   Start-Service DFSR
   ```
6. **Checking Event IDs**
   - **4614** → SYSVOL initialized (Non-Authoritative DC)
   - **4602** → Replication started and synchronized successfully

Phase 1 – Authoritative Synchronization (DFSR-Based Replication)

Purpose:

To restore SYSVOL replication across all domain controllers when DFSR (Distributed File System Replication) has stopped or become inconsistent.
This phase ensures that all DCs receive the latest Group Policy and SYSVOL data from the most up-to-date domain controller (Authoritative DC).

Step 1 – Identify Replication Failure

1. Check the **Event Viewer** on all domain controllers under:
   `Applications and Services Logs → DFS Replication`
2. Look for **Event ID 4012**, which indicates that **DFSR has stopped** due to a replication error or mismatch.
3. Confirm which DC has the **latest and most complete SYSVOL/Policies** folder.
   This DC will serve as the **Authoritative Synchronization Source** (e.g., `VNKN01-ADS-01`).

Step 2 – Stop DFS Replication Service on All DCs

Run the following command on each domain controller (run PowerShell as Administrator):

```
# Stop the DFS Replication service
Stop-Service -Name DFSR -Force
```

Step 3 – Disable DFS Replication (msDFSR-Enabled = FALSE)

Use ADSI Edit or PowerShell to manually set the DFSR attribute to disable replication on all DCs.
PowerShell Example:

```
# Example: Disable DFSR on all DCs
Set-ADObject -Identity "CN=SYSVOL Subscription, CN=Domain System Volume, CN=DFSR-
LocalSettings, CN=VNKN01-ADS-01 OU=Domain Controllers, DC=VNKN01, DC=local" `
-Replace @{msDFSR-Enabled=$false}
```

***Note:** After disabling replication, **Event IDs 2010 and 4114** should appear, confirming SYSVOL replication is disabled.*

Step 4 – Configure Authoritative Domain Controller

On the selected Authoritative DC (e.g., VNKN01-ADS-01):

```
# Set msDFSR-Options to 1 (mark as authoritative)
Set-ADObject -Identity "CN=SYSVOL Subscription, CN=Domain System Volume, CN=DFSR-
LocalSettings, CN=VNKN01-ADS-01, OU=Domain Controllers, DC=VNKN01, DC=local" `
-Replace @{msDFSR-Options=1}
```

On all DCs (including the authoritative one), re-enable DFSR:

```
# Re-enable DFSR replication
Set-ADObject -Identity "CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-
LocalSettings,CN=<DCName>,OU=Domain Controllers,DC=VNKN01,DC=local" `
-Replace @{msDFSR-Enabled=$true}
```

Step 5 – Start DFS Replication Service

Start the DFS Replication service on all DCs:

```
Start-Service -Name DFSR
Get-SmbShare -Name SYSVOL, NETLOGON
```

Step 6 – Monitor Event Logs

After the service starts, check **Event Viewer → DFS Replication Logs** for the following:

Event ID	Meaning
4602	Replication initialized successfully on the **Authoritative DC.**
4614	SYSVOL has been successfully synchronized on the **non-authoritative DCs.**

> Once these events appear, SYSVOL replication is restored and consistent across all domain controllers.

Step 7 – Verify SYSVOL and NETLOGON Shares

Confirm that the SYSVOL and NETLOGON shares have been recreated successfully:

```powershell
Get-SmbShare -Name SYSVOL, NETLOGON
```

Expected Output:

```pgsql
Name      ScopeName Path                                      Description
----      --------- ----                                      -----------
NETLOGON  *         C:\Windows\SYSVOL\sysvol\VNKN01.local\scripts Logon server share
SYSVOL    *         C:\Windows\SYSVOL\sysvol                  Logon server share
```

✅ **Result:**

All Domain Controllers (VNKN01-ADS-01, VNKN01-ADS-02, and VNKN01-ADS-03) now have:

- Identical **SYSVOL** and **Policy Template** folders
- Fully functional DFSR-based replication
- Restored **SYSVOL** and **NETLOGON** shares

Phase 2: Fix The Issue of SYSVOL Replication Breakdown with PowerShell cmdlet.

Step 1 – Check DFSR State on Each DC

1. Run the following command on each domain controller:
   dfsrdiag pollad
2. This forces DFSR to read configuration data from Active Directory immediately.
   - Then check replication status:
     dfsrdiag ReplicationState
3. This will show whether SYSVOL replication is in progress or halted.

Step 2 – Rebuild Missing SYSVOL/NETLOGON Shares

1. If shares are still missing even after restarting DFSR and Netlogon:

   Stop DFSR Service
   Stop-Service -Name DFSR

2. Rename Existing SYSVOL Folder (if corrupted)

   Rename-Item "C:\Windows\SYSVOL\sysvol" "sysvol.old"

3. Recreate a Clean SYSVOL Folder

   New-Item -ItemType Directory -Path "C:\Windows\SYSVOL\sysvol\<VNKN01.local>"

4. Start DFSR Service

   Start-Service -Name DFSR

5. Restart Netlogon Service to Recreate Shares

   Restart Service -Name Netlogon

   Verify SYSVOL and NETLOGON Shares

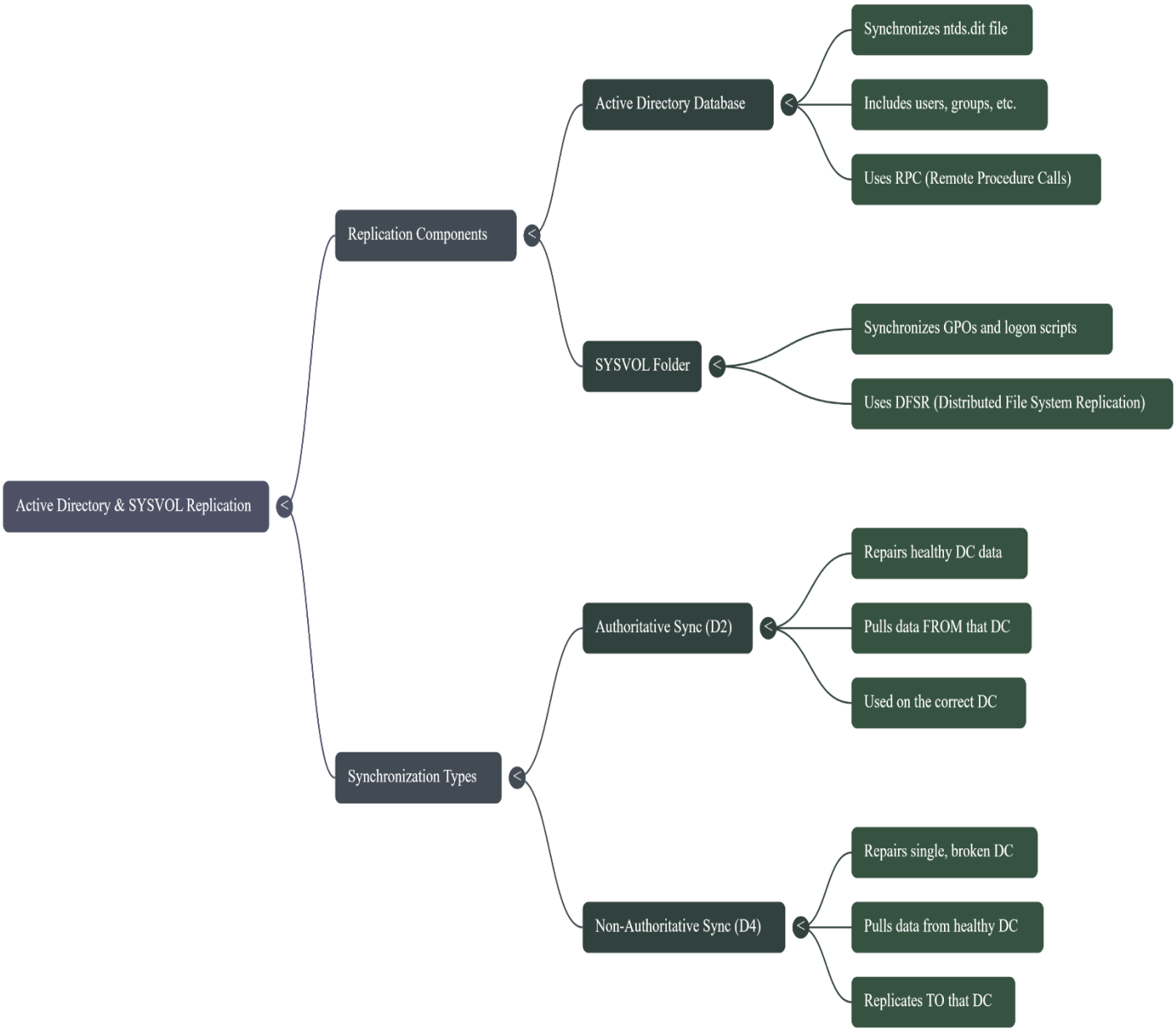
   Get-SmbShare -Name SYSVOL, NETLOGON

   Note: If replication resumes successfully, you should now see both shares listed.

Step 6 – Validate Event Logs

Check Event Viewer → Applications and Services Logs → DFS Replication

1. Event ID 4602 → Replication initialized (authoritative DC)
2. Event ID 4614 → SYSVOL successfully synchronized and


Active Directory & SYSVOL Replication
Replication Components
Active Directory Database
Synchronizes ntds.dit file
Includes users, groups, etc.
Uses RPC (Remote Procedure Calls)
SYSVOL Folder
Synchronizes GPOs and logon scripts
Uses DFSR (Distributed File System Replication)
Synchronization Types
Authoritative Sync (D2)
Repairs healthy DC data
Pulls data FROM that DC
Used on the correct DC
Non-Authoritative Sync (D4)
Repairs single, broken DC
Pulls data from healthy DC
Replicates TO that DC