How to Perform Authoritative Sync of SYSVOL Data Using Distributed File System Replication (DFS)

Instructions

> **Important:** This article is only applicable if SYSVOL data is being replicated using Distributed File System Replication (DFSR). This has been the preferred method of replicating SYSVOL data since Windows Server 2008. It is possible, however, that the older method, File Replication Service (FRS), is still in use if the domain has existed for a long time. To determine whether DFSR is in use, run `dfsrmig /getmigrationstate` from an elevated command prompt on a domain controller (DC). If the migration state is "Eliminated," DFSR is in use.

The SYSVOL folder hierarchy, present on all Active Directory DCs, is used to store two important sets of data:

- Group Policy template files: These are stored in separate folders beneath `\\SYSVOL\<domain>\Policies`.
- Log on, log off, startup, and shutdown scripts used by machines in the domain: These are stored in `\\SYSVOL\<domain>\scripts`. The **scripts** folder is itself shared as NETLOGON.

This data is replicated among DCs, but SYSVOL replication takes place separately from Active Directory replication. It is possible for one to fail while the other is fully functional. In some situations, SYSVOL replication may fail and be unable to resume without manual intervention. The following steps perform an *authoritative* sync of SYSVOL. In an authoritative sync, DFSR initializes SYSVOL using the DC's own copy of the SYSVOL data. This becomes the source copy of SYSVOL for the domain. An authoritative sync is necessary if the DC with the most up-to-date copy of the SYSVOL data is the DC on which DFSR has stopped working. This is implicitly true if there is only one DC in the domain.

Instructions for performing a non-authoritative sync of SYSVOL data using DFSR can be found in How to Perform a Non-Authoritative Sync of SYSVOL Data Using Distributed File System Replication (DFSR).

Note: This article does not specify which DC should be chosen as authoritative. Doing so can take some time, especially in a large domain. It requires examining the SYSVOL data on each DC and determining which DC has the most complete and up-to-date data. The process below begins **after** an authoritative DC has been chosen.

To perform an authoritative sync of SYSVOL data using DFSR, follow these steps:

1. On the authoritative DC, launch the ADSI Edit console (`adsiedit.msc`).
2. If the **Default naming context** is already listed in the left pane, go to the next step. Otherwise, perform the following steps to connect to the default naming context:
    1. Right-click the **ADSI Edit** header in the left pane and select **Connect to…**.
    2. Select the radio button labeled **Select a well known Naming Context** and select **Default naming context** from the dropdown list.
    3. Click **OK**. The **default naming context** should now appear in the left pane of the console.
3. Under the default naming context, browse to **DC=*domain* > OU=Domain Controllers > CN=*servername* > CN=DFSR-LocalSettings > CN=Domain System Volume**. In this step, **servername** represents the name of the DC that has been chosen as authoritative.
4. Right-click **CN=SYSVOL Subscription** and select **Properties**.
5. Double-click the **msDFSR-Enabled** attribute and set its value to **FALSE**.
6. Double-click the **msDFSR-Options** attribute and set its value to **1**.
7. Click **OK** to close the properties window.
8. Repeat steps 3-5, *but not step 6*, replacing **servername** with the name of every other DC in the domain. In other words, browse to the **CN=SYSVOL Subscription** object of each of the other DCs and set its **msDFSR-Enabled** attribute to **FALSE.** Do not change the value of the **msDFSR-Options** attribute.
9. Force Active Directory replication throughout the domain. This may take some time, depending on the size and replication topology of the domain.
10. On every DC in the domain, run `dfsrdiag pollad` from an elevated command prompt.
11. On the authoritative DC, launch Event Viewer and confirm that the DFS Replication event log contains event 4114. This event indicates that SYSVOL is no longer being replicated. (This event is present on all DCs, but checking all of them is not necessary.)
12. In ADSI Edit, browse to the location in step 3 and set the **msDFSR-Enabled** attribute to **TRUE**.
13. On the authoritative DC, run `dfsrdiag pollad` from an elevated command prompt.
14. Check the DFS Replication event log from the authoritative DC for event 4602. This event confirms that an authoritative sync of SYSVOL has occurred on this DC.
15. Repeat step 8, but set each DC's **msDFSR-Enabled** attribute to **TRUE** this time. As before, do not change the value of the **msDFSR-Options** attribute.
16. Force Active Directory replication throughout the domain.
17. On every DC except the authoritative DC, run `dfsrdiag pollad` one last time.
18. On at least one of the non-authoritative DCs, confirm that events 4614 and 4604 appear in the DFS Replication event log. These events indicate that those DCs have performed a non-authoritative sync of SYSVOL.

The steps above ensure that a non-authoritative sync of SYSVOL is performed on all other DCs after the authoritative sync is performed on the authoritative DC. This avoids possible conflicts arising in the SYSVOL data.

Additional Information

If the `dfsrdiag pollad` command is not recognized, you have two options:

- Restart the DFS Replication service instead of running the command. If other (non-SYSVOL) data are replicated by DFSR, this may cause brief interruptions.
- Install the DFS Management tools by selecting **Add Roles and Features** from the **Manage** menu of Server Manager. The DFS Management tools are found at the location shown below.

Windows Server manager Add Features Selection Screen

Revision #1
Created 2026-01-16 14:20:28 UTC by Ryan
Updated 2026-01-16 14:22:22 UTC by Ryan