How to force authoritative and non-authoritative synchronization for DFSR-replicated sysvol replication

https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/force-authoritative-non-authoritative-synchronization#how-to-perform-an-authoritative-synchronization-of-dfsr-replicated-sysvol-replication-like-d4-for-frs

Summary

Consider the following scenario:

You want to force the non-authoritative synchronization of sysvol replication on a domain controller (DC). In the File Replication Service (FRS), it was controlled through the **D2** and **D4** data values for the `Bur Flags` registry values, but these values don't exist for the Distributed File System Replication (DFSR) service. You can't use the DFS Management snap-in (Dfsmgmt.msc) or the Dfsradmin.exe command-line tool to achieve this. Unlike custom DFSR replicated folders, sysvol replication is intentionally protected from any editing through its management interfaces to prevent accidents.

How to perform a non-authoritative synchronization of DFSR-replicated sysvol replication

(like D2 for FRS)

1. In the ADSIEDIT.MSC tool, modify the following distinguished name (DN) value and attribute on each of the domain controllers (DCs) that you want to make non-authoritative:

   Console Copy

   ```
   CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain>

   msDFSR-Enabled=FALSE
   ```

2. Force Active Directory replication throughout the domain.
3. Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:

   Console Copy

   ```
   DFSRDIAG POLLAD
   ```

4. You'll see Event ID 4114 in the DFSR event log indicating sysvol replication is no longer being replicated.
5. On the same DN from Step 1, set **msDFSR-Enabled=TRUE**.
6. Force Active Directory replication throughout the domain.
7. Run the following command from an elevated command prompt on the same servers that you set as non-authoritative:

   Console Copy

   ```
   DFSRDIAG POLLAD
   ```

8. You'll see Event ID 4614 and 4604 in the DFSR event log indicating sysvol replication has been initialized. That domain controller has now done a **D2** of sysvol replication.

How to perform an authoritative synchronization of DFSR-replicated sysvol replication (like D4 for FRS)

1. Set the DFS Replication service Startup Type to Manual, and stop the service on all domain controllers in the domain.
2. In the ADSIEDIT.MSC tool, modify the following DN and two attributes on the domain controller you want to make authoritative (preferably the PDC Emulator, which is usually the most up-to-date for sysvol replication contents):

   Console Copy

   ```
   CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain>

   msDFSR-Enabled=FALSE
   msDFSR-options=1
   ```

3. Modify the following DN and single attribute on **all** other domain controllers in that domain:

   Console Copy

   ```
   CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<each other server name>,OU=Domain Controllers,DC=<domain>

   msDFSR-Enabled=FALSE
   ```

4. Force Active Directory replication throughout the domain and validate its success on all DCs.
5. Start the DFSR service on the domain controller that was set as authoritative in Step 2.
6. You'll see Event ID 4114 in the DFSR event log indicating sysvol replication is no longer being replicated.
7. On the same DN from Step 2, set **msDFSR-Enabled=TRUE**.
8. Force Active Directory replication throughout the domain and validate its success on all DCs.
9. Run the following command from an elevated command prompt on the same server that you set as authoritative:

   Console Copy

   ```
   DFSRDIAG POLLAD
   ```

10. You'll see Event ID 4602 in the DFSR event log indicating sysvol replication has been initialized. That domain controller has now done a **D4** of sysvol replication.
11. Start the DFSR service on the other non-authoritative DCs. You'll see Event ID 4114 in the DFSR event log indicating sysvol replication is no longer being replicated on each of them.

12. Modify the following DN and single attribute on **all** other domain controllers in that domain:

    Console Copy

    ```
    CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<each other server name>,OU=Domain Controllers,DC=<domain>

    msDFSR-Enabled=TRUE
    ```

13. Run the following command from an elevated command prompt on all non-authoritative DCs (that is, all but the formerly authoritative one):

    Console Copy

    ```
    DFSRDIAG POLLAD
    ```

14. Return the DFSR service to its original Startup Type (Automatic) on all DCs.

More information

If setting the authoritative flag on one DC, you must non-authoritatively synchronize all other DCs in the domain. Otherwise you'll see conflicts on DCs, originating from any DCs where you did not set auth/non-auth and restarted the DFSR service. For example, if all logon scripts were accidentally deleted and a manual copy of them was placed back on the PDC Emulator role holder, making that server authoritative and all other servers non-authoritative would guarantee success and prevent conflicts.

If making any DC authoritative, the PDC Emulator as authoritative is preferable, since its sysvol replication contents are most up to date.

The use of the authoritative flag is only necessary if you need to force synchronization of all DCs. If only repairing one DC, make it non-authoritative and don't touch other servers.

This article is designed with a 2-DC environment in mind, for simplicity of description. If you had more than one affected DC, expand the steps to include ALL of them as well. It also assumes you have the ability to restore data that was deleted, overwritten, damaged, and so on. previously if it's a disaster recovery scenario on all DCs in the domain.

Revision #1
Created 25 October 2024 14:45:59 by ColtM
Updated 25 October 2024 14:46:36 by ColtM