Non-Authoritative and Authoritative SYSVOL Restore (DFS Replication)

rebeladmin.com/non-authoritative-authoritative-sysvol-restore-dfs-replication

Dishan M. Francis August 14, 2017

Healthy SYSVOL replication is key for every active directory infrastructure. when there is SYSVOL replication issues you may notice,

1. Users and systems are not applying their group policy settings properly.

2. New group policies not applying to certain users and systems.

3. Group policy object counts is different between domain controllers (inside SYSVOL folders)

4. Log on scripts are not processing correctly

Also, same time if you look in to event viewer you may able to find events such as,

Event Id	Event Description
2213	The DFS Replication service stopped replication on volume C:. This occurs when a DFSR JET database is not shut down cleanly and Auto Recovery is disabled. To resolve this issue, back up the files in the affected replicated folders, and then use the ResumeReplication WMI method to resume replication. Recovery Steps 1. Back up the files in all replicated folders on the volume. Failure to do so may result in data loss due to unexpected conflict resolution during the recovery of the replicated folders. 2. To resume the replication for this volume, use the WMI method ResumeReplication of the DfsrVolumeConfig class. For example, from an elevated command prompt, type the following command: wmic /namespace:\\root\microsoftdfs path dfsrVolumeConfig where volumeGuid=”xxxxxxxx″ call ResumeReplication
5002	The DFS Replication service encountered an error communicating with partner <FQDN> for replication group Domain System Volume.
5008	The DFS Replication service failed to communicate with partner <FQDN> for replication group Home-Replication. This error can occur if the host is unreachable, or if the DFS Replication service is not running on the server.

5014	The DFS Replication service is stopping communication with partner <FQDN> for replication group Domain System Volume due to an error. The service will retry the connection periodically.

Some of these errors can be fixed with simple server reboot or running commands describe in the error (ex – event 2213 description) but if its keep continuing we need to do Non-Authoritative or Authoritative SYSVOL restore.

Non-Authoritative Restore

If it's only one or few domain controller (less than 50%) which have replication issues in a given time, we can issue a non-authoritative replication. In that scenario, system will replicate the SYSVOL from the PDC.

Authoritative Restore

If more than 50% of domain controllers have SYSVOL replication issues, it possible that entire SYSVOL got corrupted. In such scenario, we need to go for Authoritative Restore. In this process, first we need to restore SYSVOL from backup to PDC and then replicate over or force all the domain controllers to update their SYSVOL copy from the copy in PDC.

SYSVOL can replicate using FRS too. This is deprecated after windows server 2008, but if you migrated from older Active Directory environment you may still have FRS for SYSVOL replication. It also supports for Non-Authoritative and Authoritative restore but in this demo, I am going to talk only about SYSVOL with DFS replication.

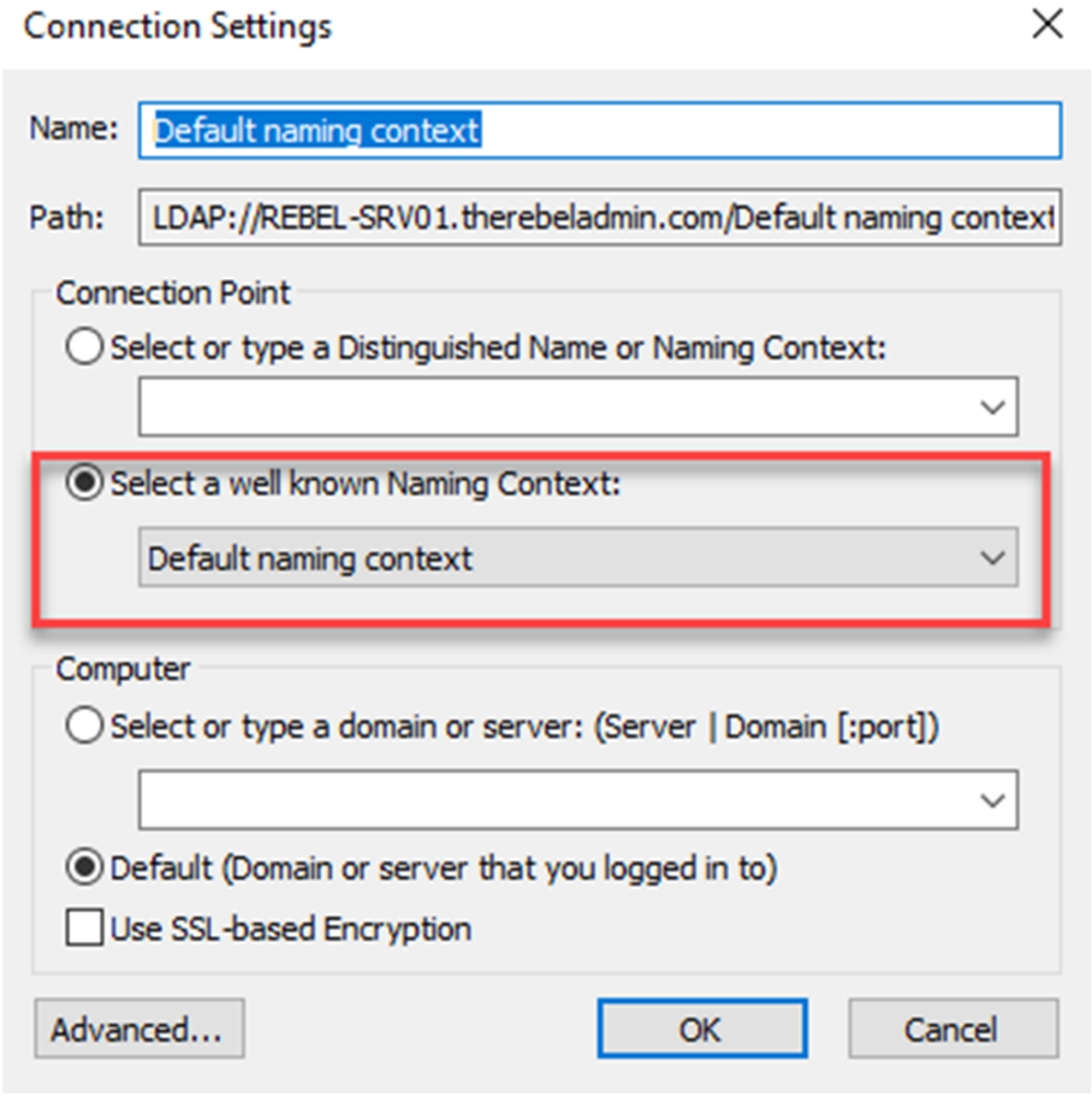
Non-Authoritative DFS Replication

In order to perform a non-authoritative replication,

1) Backup the existing SYSVOL – This can be done by copying the SYSVOL folder from the domain controller which have DFS replication issues in to a secure location.

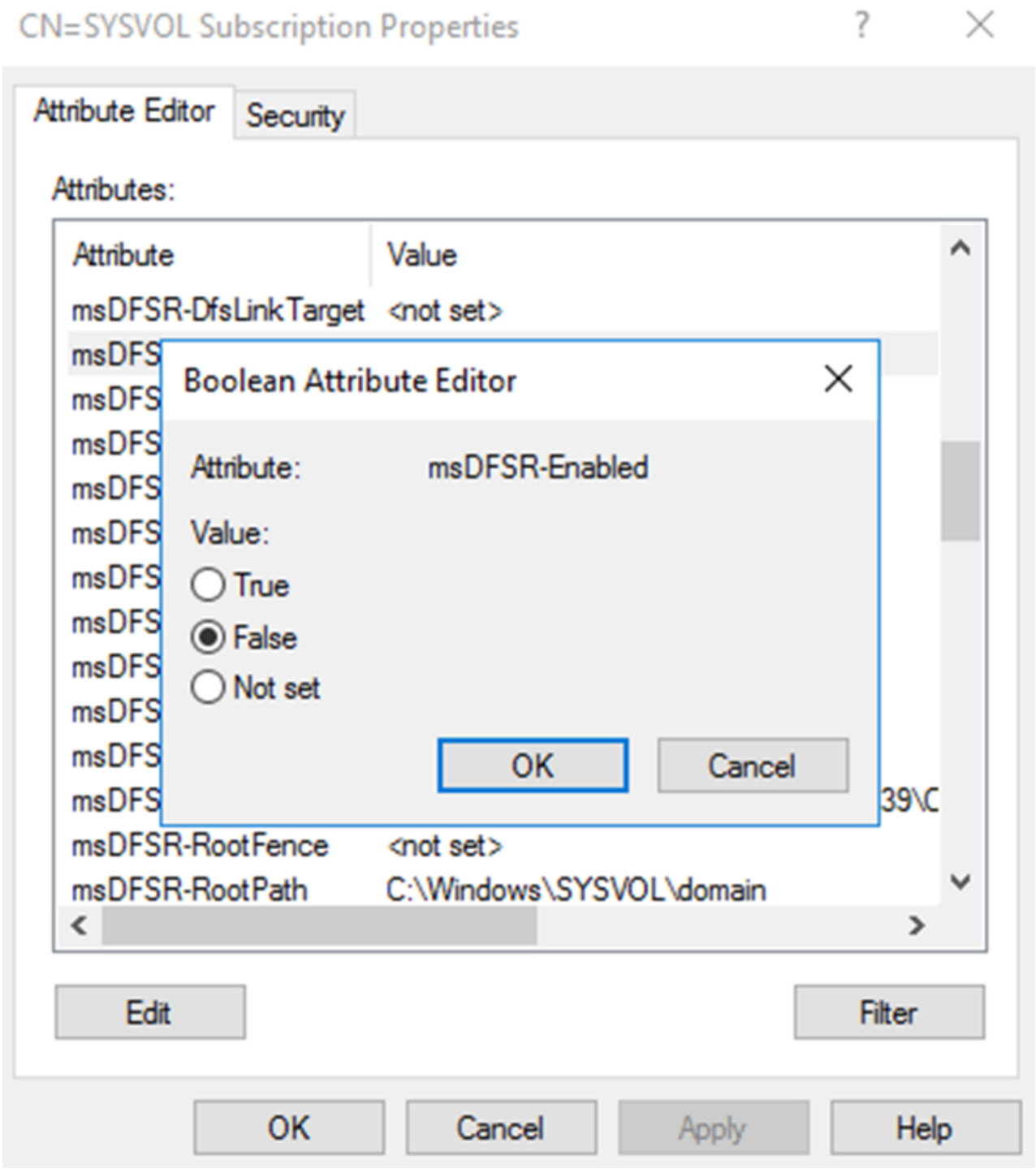
2) Log in to Domain Controller as Domain Admin/Enterprise Admin

3) Launch **ADSIEDIT.MSC** tool and connect to Default Naming Context



4) Brows to **DC=domain,DC=local > OU=Domain Controllers > CN=(DC NAME) > CN=DFSR-LocalSettings > Domain System Volume > SYSVOL Subscription**

5) Change value of attribute **msDFSR-Enabled = FALSE**



6) Force the AD replication using,

repadmin /syncall /AdP

7) Run following to install the DFS management tools using (unless this is already installed),

Add-WindowsFeature RSAT-DFS-Mgmt-Con

8) Run following command to update the DFRS global state,

dfsrdiag PollAD

9) Search for the event **4114** to confirm SYSVOL replication is disabled.

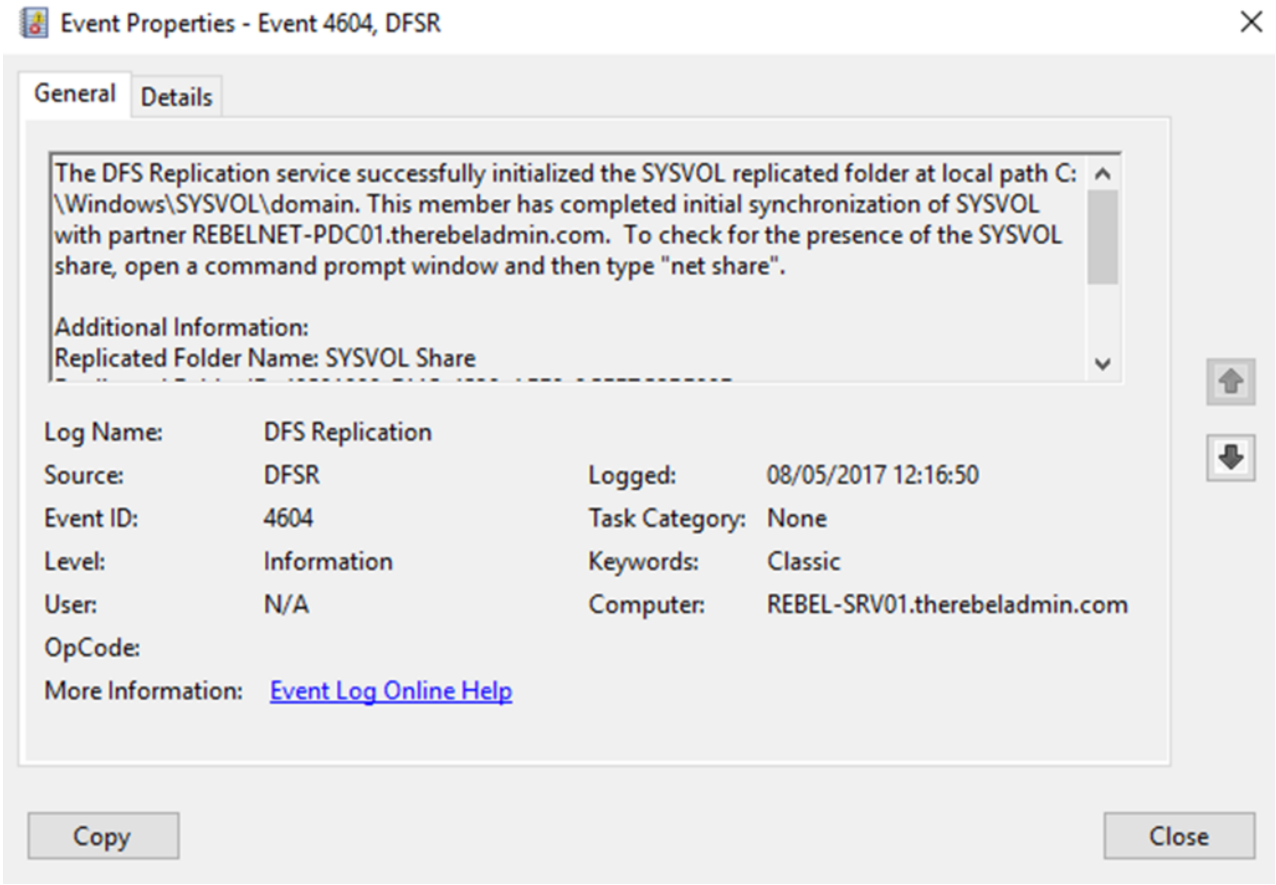
Get-EventLog -Log "DFS Replication" | where {$_.eventID -eq 4114} | fl

10) Change the attribute value back to **msDFSR-Enabled=TRUE** (step 5)

11) Force the AD replication as in step 6

12) Update DFRS global state running command in step 8

13) Search for events **4614** and **4604** to confirm successful non-authoritative synchronization.



All these commands should run from domain controllers set as non-authoritative.

Authoritative DFS Replication

In order to perform to initiate authoritative DFS Replication,

1) Log in to PDC FSMO role holder as Domain Administrator or Enterprise Administrator

2) Stop DFS Replication Service (This is recommended to do in all the Domain Controllers)

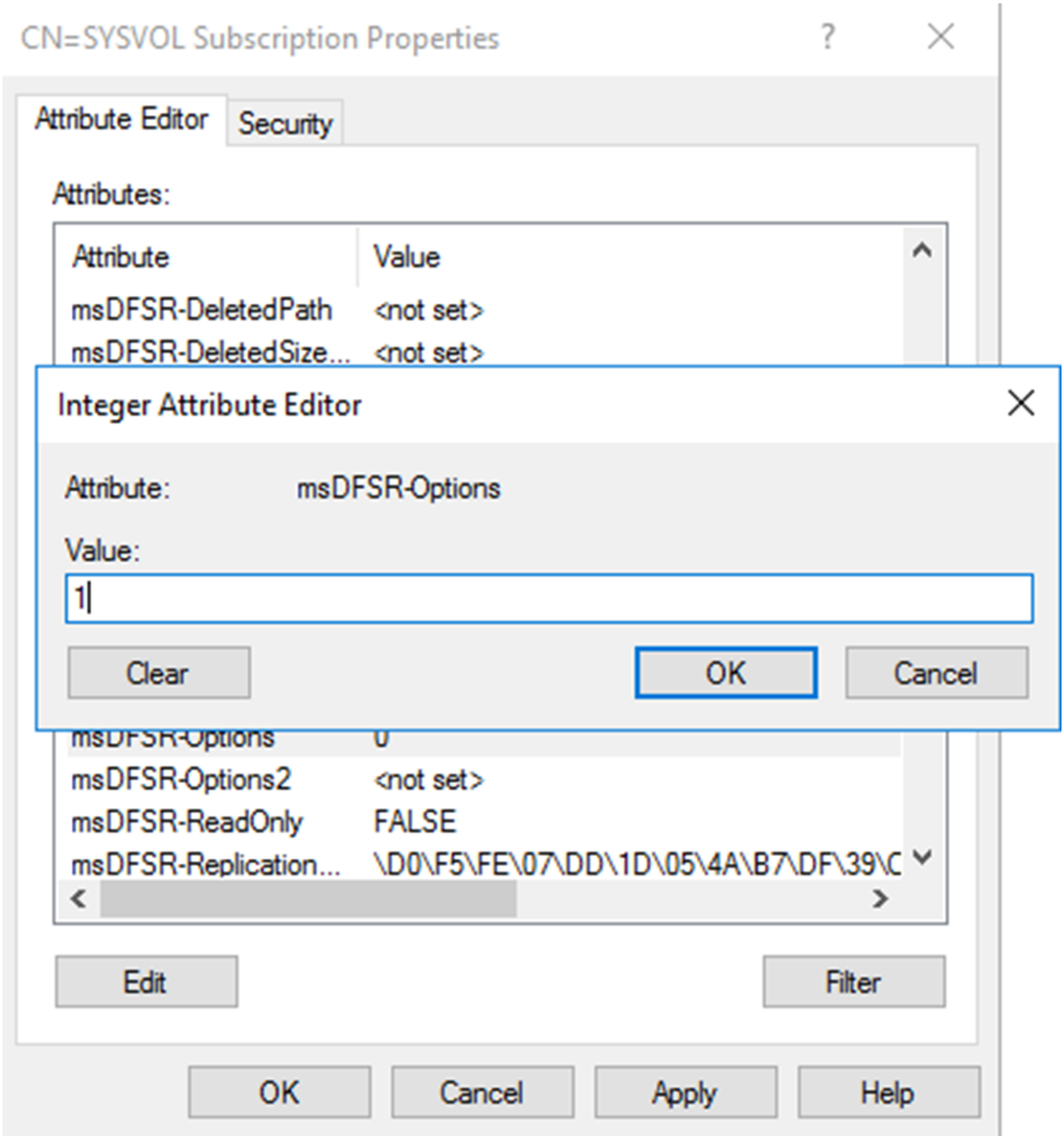
3) Launch **ADSIEDIT.MSC** tool and connect to Default Naming Context

4) Brows to **DC=domain,DC=local > OU=Domain Controllers > CN=(DC NAME) > CN=DFSR-LocalSettings > Domain System Volume > SYSVOL Subscription**

5) Update the given attributes values as following,

msDFSR-Enabled=FALSE

msDFSR-options=1



6) Modify following attribute on ALL other domain controller.

msDFSR-Enabled=FALSE

7) Force the AD replication using,

repadmin /syncall /AdP

8) Start DFS replication service in PDC

9) Search for the event **4114** to verify SYSVOL replication is disabled.

10) Change following value which were set on the step 5,

msDFSR-Enabled=TRUE

11) Force the AD replication using,

repadmin /syncall /AdP

12) Run following command to update the DFRS global state,

dfsrdiag PollAD

13) Search for the event **4602** and verify the successful SYSVOL replication.

14) Start DFS service on all other Domain Controllers

15) Search for the event **4114** to verify SYSVOL replication is disabled.

16) Change following value which were set on the step6. This need to be done on ALL domain controllers.

msDFSR-Enabled=TRUE

17) Run following command to update the DFRS global state,

dfsrdiag PollAD

18) Search for events **4614** and **4604** to confirm successful authoritative synchronization.

Please note you do not need to run Authoritative DFS Replication for every DFS replication issue. It should be the last option.

Hope this was useful and if you have any questions feel free to contact me on **rebeladm@live.com**