How to troubleshoot missing SYSVOL and Netlogon shares

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

This article provides the steps to troubleshoot the missing `SYSVOL` and `Netlogon` shares in Windows Server 2012 R2.

Original KB number: 2958414

Symptoms

`SYSVOL` and `Netlogon` shares aren't shared on a domain controller. The following symptoms or conditions may also occur:

- The `sysvol` folder is empty.
- The affected domain controller was recently promoted.
- The environment contains domain controllers running versions of Windows earlier than Windows Server 2012 R2.
- DFS Replication is used to replicate the `SYSVOL` Share replicated folder.
- An upstream domain controller's DFS Replication service is in an error state.

Cause

Domain controllers without `SYSVOL` shared can't replicate inbound because of upstream (source) domain controllers being in an error state. Frequently (but not limited to), the upstream servers have stopped replication because of a dirty shutdown (event ID 2213).

Resolution

This section contains recommended methods for troubleshooting and resolving missing `SYSVOL` and `Netlogon` shares on domain controllers that replicate by using the DFS Replication service.

The process reinitializes DFS Replication if `SYSVOL` isn't shared on domain controllers according to How to force an authoritative, or non-authoritative synchronization for DFSR-replicated SYSVOL (like "D4/D2" for FRS). It's unnecessary in most cases, and it may cause data loss if done incorrectly. In addition, it prevents determining the cause of the issue and averting future occurrences of the issue.

What follows are general steps to investigate the missing shares. Determine if the problem is caused by a one-time occurrence, or if the upstream domain controller(s) can't support replication by using DFS Replication.

Deleting the DFS Replication database from the volume shouldn't be required and is discouraged. It causes DFS Replication to consider all local data on the server to be nonauthoritative. By letting DFS Replication recover the database gracefully (as instructed in the 2213 event), the last writer will still win any conflicting versions of `SYSVOL` data.

Step 1 - Evaluate the state of DFS Replication on all domain controllers

Evaluate how many domain controllers aren't sharing `SYSVOL`, have recently logged an Error event, and how many domain controllers are in an error state. Follow these steps.

- Check for the `SYSVOL` share
  You may manually check whether `SYSVOL` is shared or you can inspect each domain controller by using the net view command:
  Console Copy

```
For /f %i IN ('dsquery server -o rdn') do @echo %i && @(net view \\%i | find "SYSVOL") & echo
```

- Check DFS Replication state
  To check DFS Replication's state on domain controllers, you may query WMI. You can query all domain controllers in the domain for the `SYSVOL` Share replicated folder by using WMI as follows:
  Console Copy

```
For /f %i IN ('dsquery server -o rdn') do @echo %i && @wmic /node:"%i"
/namespace:\\root\microsoftdfs path dfsrreplicatedfolderinfo WHERE replicatedfoldername='SYSVOL
```

```
share' get replicationgroupname,replicatedfoldername,state
```

The `state` values can be any of:
0 = Uninitialized
1 = Initialized
2 = Initial Sync
3 = Auto Recovery
4 = Normal
5 = In Error
Note
Depending on a domain controller's condition, it may fail to report a state value and indicate no instance(s) available.

- Check Event logs for recent errors or warnings
  If any domain controllers don't report the `SYSVOL` Share replicated folder as being in a state 4 (normal), check the event log of those domain controller(s) to evaluate their condition. Review each domain controller for recent errors or warnings in the DFS Replication event log, such as the warning event ID 2213 that indicates that DFS Replication is currently paused.
- Check the Content Freshness configuration
  Determine whether DFS Replication triggered content freshness protection on the affected domain controllers. Content Freshness is enabled on Windows Server 2012 (and later versions) domain controllers by default. However, it may also be manually enabled on Windows Server 2008 R2 servers.
  To evaluate if content freshness is enabled, the `MaxOfflineTimeInDays` setting will be set to **60**. If content freshness is disabled, `MaxOfflineTimeInDays` will be set to **0**. To check `MaxOfflineTimeInDays`, run the following command:
  Console Copy

```
wmic.exe /node:%computername% /namespace:\\root\microsoftdfs path DfsrMachineConfig get MaxOfflineTimeInDays
```

To query all domain controllers in the domain, run the following command:
Console Copy

```
For /f %i IN ('dsquery server -o rdn') do @echo %i && @wmic /node:"%i" /namespace:\\root\microsoftdfs path DfsrMachineConfig get MaxOfflineTimeInDays
```

For each domain controller enabled for content freshness, evaluate if DFS Replication has logged an event ID 4012 that indicates replication of the folder has stopped because replication has failed for longer than the `MaxOfflineTimeInDays` parameter.

Step 2 - Prepare the domain controllers that are in an error state

- Install appropriate updates
  For any domain controllers running Windows Server 2008 R2, first install DFS Replication updates to prevent data loss and to fix known issues. It's a best practice to use the latest version of DFS Replication. See List of currently available hotfixes for Distributed File System (DFS) technologies for the latest version of DFS Replication.
- Back up `SYSVOL` data
  Do a backup of `SYSVOL` data (if present) on each domain controller. Backups may be a file copy of the `SYSVOL` contents to a safe location or, it may be a backup that uses backup software.
  Depending on the situation, policy files could be moved to **PreExisting** or **Conflict and Deleted**. **PreExisting** and **Conflict and Deleted** contents will be purged if initial synchronization is done multiple times on a server. Back up data in these locations to avoid data loss.

Step 3 - Recover DFS Replication on the domain controllers in the error state

Based on the number of domain controllers in the domain, select the appropriate method to recover the DFS Replication service.

For environments that have two domain controllers

Determine whether a dirty shutdown was detected (event ID 2213) on either domain controller. You may find the second domain controller is waiting to complete initialization of `SYSVOL`. The reason is, after promotion, it will log a 4614 event that indicates that DFS Replication is waiting to do initial replication. In addition, it won't log a 4604 event signaling that DFS Replication has initialized `SYSVOL`.

- If content freshness is enabled on both domain controllers
  If the second domain controller waits to do initial synchronization (event 4614 logged without the 4604 anti-event), follow the How to force an authoritative and non-authoritative synchronization for DFSR-replicated SYSVOL (like "D4/D2" for FRS) to set the first domain controller as authoritative. You don't have to configure the second domain controller as nonauthoritative, because it's already waiting to do initial synchronization.
  Or, if the second domain controller is healthy and `SYSVOL` is shared, take the following steps:
  1. Back up all `SYSVOL` contents of the first domain controller.

2. Evaluate if the second domain controller's `SYSVOL` data is up to date. If not, you may want to copy updated `SYSVOL` files to the second domain controller from the first domain controller. Otherwise, any existing data present on first domain controller not present on the second will go into the **PreExisting** and **Conflict and Deleted** folders.
3. Set the first domain controller as nonauthoritative by disabling the membership per How to force an authoritative and non-authoritative synchronization for DFSR-replicated SYSVOL (like "D4/D2" for FRS). Confirm that an event ID 4114 is logged to indicate the membership is disabled.
4. Enable the first domain controller's membership, and wait for the 4614 and 4604 events that report completion of the initial synchronization. If necessary, restore any updated files from PreExisting to the original location.

- If content freshness isn't enabled or triggered on both domain controllers
  If the first domain controller is in the event ID 2213 state, and the second domain controller has never completed initialization after it was promoted, and content freshness hasn't been triggered. Take the following steps:
  1. Run the `ResumeReplication` WMI method on the first domain controller as instructed in the 2213 event.
  2. After replication resumes, it will log an event ID 4602 that indicates that DFS Replication initialized the `SYSVOL` replicated folder and specified it as the primary member.
  3. Run the `dfsrdiag pollad` command on the second domain controller to trigger it to complete initial sync (event ID 4614). As soon as initial sync is finished, event ID 4604 is logged, signaling `SYSVOL` has completed initialization.

  Or, if the first domain controller is in the 2213 state and the second domain controller is healthy (`SYSVOL` is shared), run the `ResumeReplication` WMI method on the first domain controller. It will log event ID 2214 at the completion of dirty shutdown recovery.

For environments that have three or more domain controllers

Determine whether a dirty shutdown was detected and whether DFS Replication is paused on any domain controllers (event ID 2213). You may find a domain controller is waiting to complete initialization of `SYSVOL` after promotion. It will log a 4614 event that indicates that DFS Replication is waiting to do initial replication. It also won't log a 4604 event signaling that DFS Replication has initialized `SYSVOL`.

- If content freshness is enabled, and there are three or more domain controllers in the domain.
  Content freshness protection will log an event ID 4012 that indicates that replication has stopped because replication on the folder has failed for longer than the `MaxOfflineTimeInDays` parameter. To reinitialize DFS Replication on the affected domain controller(s), follow the instructions in How to force an authoritative and non-authoritative

synchronization for DFSR-replicated SYSVOL (like "D4/D2" for FRS).
If all domain controllers have logged the 4012 event and their state is 5, follow the instructions in How to force an authoritative and non-authoritative synchronization for DFSR-replicated SYSVOL (like "D4/D2" for FRS) to completely initialize `SYSVOL`. It's the only situation to set a DFS Replication server as authoritative. Make sure that the domain controller configured as authoritative has the most up-to-date copy of all `SYSVOL` contents.
Or, if one or more domain controllers are blocking replication because of content freshness, they each must be non-authoritatively recovered. Follow these steps:

1. Back up all `SYSVOL` contents of the domain controller(s). Typically, policy edits are done on the PDC Emulator, but it isn't guaranteed. Any data present on the recovered domain controller(s) not matching the partners will go into the **PreExisting** or **Conflict and Deleted** folder, or both.
2. Set the domain controller(s) as nonauthoritative by disabling the membership, as described in How to force an authoritative and non-authoritative synchronization for DFSR-replicated `SYSVOL` (like "D4/D2" for FRS). You must be aware of the replication topology, and you must fan out from a healthy domain controller by selecting direct partners of it, then recovering further downstream domain controllers, and so on. Event ID 4144 will be logged to confirm the membership is disabled. Make sure all domain controllers requiring recovery log the event. It may be necessary to force Active Directory replication and then run the `dfsrdiag pollad` command on each domain controller to detect the disabled membership quickly.
3. Enable the membership and wait for the 4614 and 4604 events to report completion of the initial synchronization. Restore any required files from backup or from **PreExisting** and **Conflict and Deleted** as necessary.

- If content freshness isn't enabled or triggered, and there are three or more domain controllers in the domain
  If content freshness protection isn't triggered, run the `ResumeReplication` WMI method on the affected domain controllers. You must be aware of the replication topology, and you must fan out from a healthy domain controller by selecting direct partners of it, then recovering further downstream domain controllers, and so on. After replication is resumed, DFS Replication will log events 2212, 2218, and then 2214 (indicating that DFS Replication initialized the `SYSVOL` replicated folder).

Preventing future occurrences of the issue

Check whether the Application and System event logs are frequently reporting ESENT database recovery operations, disk performance problems, or both. The event logs typically coincide with unexpected shutdowns of the system, with DFS Replication not stopping gracefully, or disk subsystem failures. Consider updating the system's drivers, installing appropriate updates to the disk subsystem, or contacting the system's hardware manufacturer to investigate further. You may also contact Microsoft Customer Support Services to help evaluate the system's health and DFS Replication behavior.

The Service Control Manager (SCM) uses the default time-out time of 20 seconds for stopping a service. In some complex DFS Replication implementations, this time-out value may be too short, and DFS Replication stops before the appropriate database is closed. At service restart, DFS Replication detects this condition, and then does the database recovery. WaitToKillServiceTimeout may be used to grant DFS Replication more time to commit changes to the database during shutdown. For more information, go to article You receive DFSR event ID 2212 after you restart the DFSR service.

After you have restored DFS Replication of `SYSVOL`, DFS Replication health must be carefully monitored in the environment to prevent this scenario. Regular review of DFS Replication event logs, collecting of DFS Replication health reports, and collecting of replication state (by using the WMI query in the Check DFS Replication state section under Step 1 - Evaluate the state of DFS Replication on all domain controllers) are recommended.

Revision #1
Created 25 October 2024 13:44:06 by ColtM
Updated 25 October 2024 13:44:38 by ColtM