**WHITEPAPER**

**Active Directory Domain Controller Upgrade Practices**

(Assessment, Plan and Upgrade)

By

Ravi Kiran Nuthi

Table of Contents

[**1.** **Introduction** 3](#_Toc146554159)

[**2.** **Assessment of Existing Forest Architecture** 3](#_Toc146554160)

[**3.** **Domain Controller Information** 3](#_Toc146554161)

[**4.** **Understanding hardware platforms and requirements** 4](#_Toc146554162)

[**4.1.** **Domain Controllers on Physical servers** 4](#_Toc146554163)

[**4.2.** **Domain Controllers on Virtualization Platforms** 4](#_Toc146554164)

[**4.3.** **Domain Controllers on Cloud platforms and WAN connectivity between sites** 4](#_Toc146554165)

[**4.4.** **Additional Domain Controllers Hardware Requirements** 5](#_Toc146554166)

[**4.5.** **Windows Server vs Server Core** 5](#_Toc146554167)

[**4.6.** **Read-Only Domain Controllers** 6](#_Toc146554168)

[**4.7.** **DNS considerations** 6](#_Toc146554169)

[**4.8.** **Firewall Ports for domains and trusts** 7](#_Toc146554170)

[**5.** **Non-Active Directory Roles and applications** 8](#_Toc146554171)

[**6.** **Domain Controller Upgrade Considerations** 8](#_Toc146554172)

[**6.1.** **Application Hardcoding** 8](#_Toc146554173)

[**6.2.** **Retain IP Address of Legacy Domain controller – platform-based considerations.** 8](#_Toc146554174)

[**6.3.** **Domain Controllers Function Levels** 9](#_Toc146554175)

[**6.4.** **NTP Settings on Domain Controllers** 11](#_Toc146554176)

[**6.5.** **FRS for domain replication (Windows 2008 Domain controllers)** 11](#_Toc146554177)

[**6.6.** **Domain Controller Upgrade checklist** 14](#_Toc146554178)

[**6.7.** **Domain Controller Demotion Checklist** 15](#_Toc146554179)

[**7.** **Remediating Issues in the Forest/Domain** 16](#_Toc146554180)

# **Introduction**

This whitepaper covers how to upgrade domain controllers (DCs) from an earlier version of Windows Server to the most recent version of Windows Server in multi-forest and multi-domain model environment and includes background information regarding Active Directory Domain Services in Windows Server.

# **Assessment of Existing Forest Architecture**

It is very essential to perform thorough assessment of existing forests and domains before carrying out legacy domain controller upgrades and document all the assessment data. Assessment generates a list of issues to address and remediate them that will help to perform domain controller upgrades without any issues.

Assessment should cover below areas in every forest and domain.

1. Domain Controller information
2. AD Sites and subnets, AD trusts
3. WAN details between sites
4. Non-AD roles information (DHCP, NPS, SMTP, WDS, Print/File Server etc)
5. Hardware information (Physical, VM, Azure and AWS)
6. Domain Controller network information (Routing and Ports)
7. Domain Controller Naming Convention information
8. DNS information
9. Active Directory replication
10. Windows Time Configuration
11. Domain joined computer Operating System Version details.
12. Domain controller backup and monitoring information
13. Issues and Risks

# **Domain Controller Information**

The Active Directory subsystem is supported by Active Directory domain controllers. Any failure of an Active Directory domain controller could affect how users, computers, and apps running in your production environment are authenticated and authorized. Thus, it is very important to gather complete information about all the domain controllers in a forest and domain.

Below details should be gathered part of every domain controller assessment

1. Operating System information
2. Networking information (IP Address, DNS, Ping and Network port)
3. Hardware details (CPU, Memory, and Disk)
4. Installed Roles and Features
5. Installed Software
6. Dcdiag status
7. DC Replication details
8. NTP configuration
9. Reachability to other domain controllers (Ping, WMI/WinRM, Other Network Ports)

# **Understanding hardware platforms and requirements**

Collect hardware details about domain controllers' hardware platforms as part of the assessment. Domain controllers are typically installed on physical servers, virtualization systems like Microsoft Hyper-V and VMware, or cloud computing services like AWS and Azure.

Majority of challenges listed below from the hardware platform point of view.

## **Domain Controllers on Physical servers**

Server hardware model may not be compatible with the latest Operating System. For example, when old HP/Dell models are compatible with Windows 2012 server, but not with Windows 2019 or Windows 2022 Server operating system, it requires to get a new physical server for building new domain controller or need to find any other hardware platform or cloud platform to get a new domain controller.

When physical server is not compatible with latest operating systems versions, then it requires further planning to get new domain controller with latest operating system considering standard procedures that customer follows. If incompatible physical hardware needs to be replaced with new physical hardware or other virtualization or cloud platforms need to be taken into consideration to acquire a new build for domain controller, project team should discuss this with customer.

In some situations, due to few challenges, it may be difficult to get new physical hardware or virtualization/cloud platforms for the building of new domain controllers in a few remote sites and this may influence project planning and timelines, so have complete clarity about challenges and difficulties, and update such events as a risk and update the risk log and discuss about it with the customer how it impacts project planning and timelines.

Take appropriate decision and action to get a new domain controller in such problematic sites to mitigate impact on project planning and timelines.

## **Domain Controllers on Virtualization Platforms**

Domain controllers with Legacy platforms may run on VMWare or Hyper-V or any other virtualization platforms. Every virtualization platform has guest OS compatibility, so part of the assessment process gathers information about existing virtualization platforms whether they are compatible with latest version of window operating system for building domain controller.

Sometimes new builds for domain controller cannot be deployed due to few challenges listed below. Discuss with the customer regarding those challenges and draft appropriate actions to get new domain controllers in the environment in such scenarios that helps to satisfy project requirements.

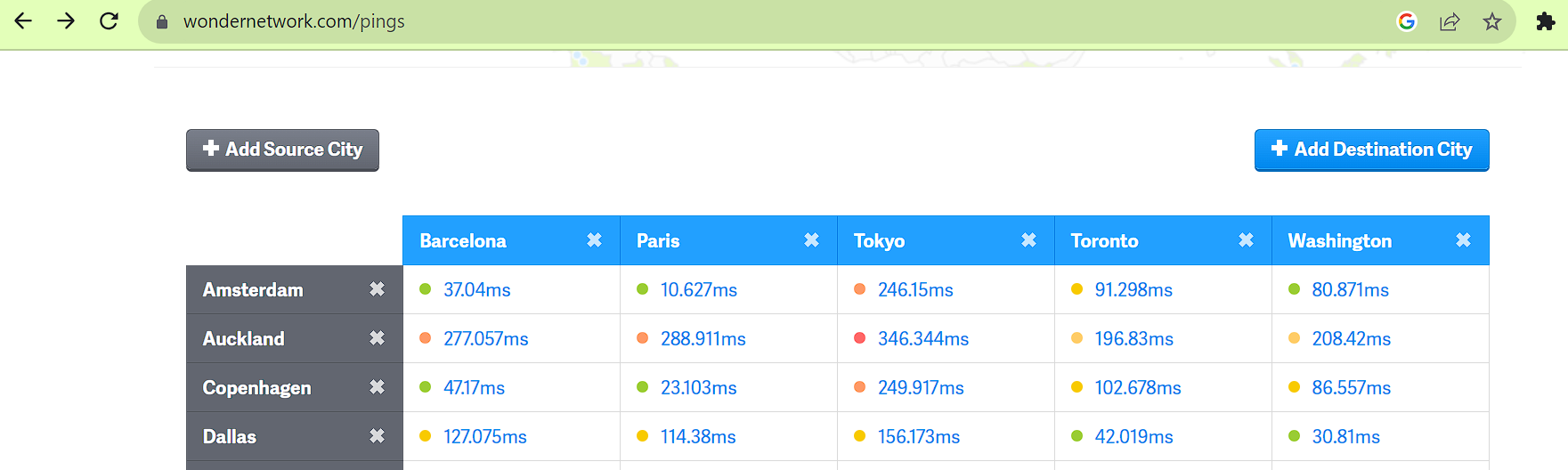
* When virtualization platform is not compatible with latest version of window operating system
* Lacking hardware resources in virtualization platforms (CPU/Memory or Disk) in other words, due to over utilization in Virtualization layer, getting new build for domain controller is challenging task for platform teams.

## **Domain Controllers on Cloud platforms and WAN connectivity between sites**

Gather legacy domain controller information those are running on cloud platforms such as Azure and AWS. Since cloud providers update underlying hardware on periodic basis, all latest version of windows operating systems can be deployed in any cloud platform and part of the assessment process, it is necessary to document about domain controller regions and the latency between the user/application environment and the region on which domain controllers are running.

For example, below website shows the ping latency between different cities and it can be used to calculate the latency between cloud regions and user/application environments.

<https://wondernetwork.com/pings>



## **Additional Domain Controllers Hardware Requirements**

When planning hardware requirements for additional domain controller, it is recommended to have thorough understanding about the environment. Basically, domain controller capacity is planned based on the number of users in a domain along with the FSMO roles configured.

Take into account Microsoft's recommendations for the hardware needed for the deployment of the Windows operating system in any environment, along with that consider other recommendations suggested by Microsoft to get an additional hardware that is required for deploying additional controller in the domain.

Refer below link for Operating System hardware requirements.

<https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements>

Below table is a rough estimate taken from MS recommendations and for more details you can refer below link

<https://learn.microsoft.com/en-us/windows-server/administration/performance-tuning/role/active-directory-server/capacity-planning-for-active-directory-domain-services#goals-of-capacity-planning>

|  |  |  |  |
| --- | --- | --- | --- |
| **Object Count** | **CPU Count** | **CPU Clock** | **Physical RAM** |
| 1-499 | One | 1 x 850 MHz | 512MB |
| 500-999 | One | 2 x 850 MHz | 1GB |
| 1000-2999 | Two | 2 x 850 MHz | 2GB |
| 3000-10000 | Two | 4 x 850 MHz | 2GB |
| > 10000 | One per 5000 users | 4 x 850 MHz | 2GB |

**NOTE:** Standard configuration is – 2 CPUs, 4GB RAM and 100GB disk is sufficient to run domain controllers in any environment without any issues unless there any other requirements.

## **Windows Server vs Server Core**

Server core do not have Graphical User interface and using server core you can deploy essential services to run specific roles and features. Since Server Core do not have GUI, it can be managed through command line, PowerShell, or remote tools. Sometimes it is difficult for few of the administrators who does not have experience in using commands.

Since Desktop Experience feature isn’t available and installed, it reduces file size on the disk and eliminates many services that are usually require by GUI. Because of its limited features, it has reduced surface attacks so less likely to be compromised, so requires fewer hot fixes, less disk and memory usage.

So, it is recommended to get server core build for new additional domain controller deployment that increases server performance.

## **Read-Only Domain Controllers**

You can set up Read Only Domain Controllers (RODC) in branch office or distant locations, which often have fewer users, a poor network, insufficient physical protection, and staff with less IT expertise. The implementation of RODC improves security and facilitates quicker access to network resources.

## **DNS considerations**

You can certainly state that DNS is essential to Active directory environments and that nothing would function properly without it. Each domain controller has a DNS role and maintains all of the domain environment’s DNS records. Name resolution essentially plays a significant role whenever a domain controller wants to communicate with another domain controller, with a PDC within the domain network, or whenever a domain joined computer or any application wants to communicate with the domain or domain controllers, other computers, or other applications.

Stale or incorrect records in DNS create risk to the AD domain operations that may include replication issues between domain controllers, applications may not authenticate domain correctly etc. So before performing domain controller upgrade activity, you must ensure that DNS and its records are in healthy state. In some scenarios, DNS will run on IPAM appliances such as Infoblox, Bluecat etc. mostly these appliances are managed by network team, so work with them to streamline DNS records when you will work on domain controller upgrades.

These IPAM tools should be configured rightly to obtain dynamic DNS updates from the domain controllers or from the domain joined computers without any manual work. In case of manual work, you need to provide DNS records of newly deployed domain controller to the network team, so that they can update records in their IPAM tool.

You can find below records for every domain controller in C:\Windows\System32\Config\netlogon.dns file which should be stored compulsory in DNS.

|  |  |
| --- | --- |
| **Record Name** | **Description** |
| ldap.\_tcp.DnsDomainName. | Allows a client to locate servers running the LDAP service in the domain of DnsDomainName. |
| \_ldap.\_tcp. SiteName.\_sites. | Allows a client to locate servers running the LDAP service in a domain in a site SiteName DnsDomainName. SiteName relative file name, which is stored in the Configuration container in Active Directory. |
|  |
| DnsDomainName. |
| \_ldap.\_tcp.dc.\_msdcs.DnsDomainName. | Allows a client to find a domain controller in the domain DnsDomainName. All DC register this SRV record. |
| \_ldap.\_tcp. SiteName. \_sites.dc.\_msdcs.DnsDomainName. | Allows a client to find a domain controller in the domain in site SiteName DnsDomainName. All DC register this SRV record. |
| \_ldap.\_tcp.pdc.\_msdcs.DnsDomainName. | Allows a client to find a domain PDC DnsDomainName. Only PDC server registers this SRV record. |
| **Record Name** | **Description** |
| \_ldap.\_tcp. SiteName. \_sites.gc.\_msdcs. DnsForestName. | Allows a client to find a GC in the forest Only GC server DnsForestName. owned by this forest register this SRV record |
| \_gc.\_tcp.DnsForestName. | Allows a client to find a GC in the domain. Only GC servers owned by this forest DnsForestName register this SRV record. |
| \_gc.\_tcp.SiteName.\_sites.DnsForestName. | Allows a client to find a GC in this forest site SiteName DnsForestName. Only GC servers owned by this forest DnsForestName register this SRV record. |
| \_ldap.\_tcp. DomainGuid.domains.\_msdcs. DnsForestName. | Allows customers to find the DC GUID. A GUID is a 128-bit unique index. Admits when DnsDomainName DnsForestName and changed. |
| \_kerberos.\_tcp. DnsDomainName . | Allows clients to find a Kerberos KDC in that domain: DnsDomainName. All DC register this SRV record. |
| \_kerberos.\_udp. DnsDomainName . | Same as \_kerberos .\_tcp. DnsDomainName only over UDP |
| \_kerberos.\_tcp.SiteName.\_sites. DnsDomainName. | Allows clients to find a Kerberos KDC in that domain: DnsDomainName site SiteName. All DC register this SRV record. |
| \_kerberos.\_tcp.dc.\_msdcs.DnsDomainName. | Allows clients to find a DC running a Kerberos KDC's role in that domain: DnsDomainName. All DC with the KDC log this SRV record. |
| \_kerberos.tcp.SiteName.\_sites.dc.\_msdcs. DnsDomainName. | Allows clients to find a DC running a Kerberos KDC's role in that domain: DnsDomainName site SiteName. All DC with the KDC log this SRV record. |
| \_kpasswd.\_tcp.DnsDomainName. | Kerberos Password Change allows you to search for current domain. All kerberos KDC DC (c) role of the register this SRV record |
| \_kpasswd.\_udp.DnsDomainName. | Same as \_kpassword .\_tcp. DnsDomainName only over UDP |

In case of any issues in the Domain environment due to some reasons in specific scenarios, you can take reference of above to validate DNS records of Domain controllers.

## **Firewall Ports for domains and trusts**

Firewall allows and disallows traffic by unblocking network ports between two subnets or between two IP Addresses and firewall is managed by Security team in many organizations.

When your domain controllers’ part of same subnet, then you do not require to contact Security team to allow traffic between domain controller unless some firewall rules are defined inside subnet, but it is really a rare situation, because all ports are opened within any network subnet and do not require to contact security team to allow network ports.

When domain controllers are running in multiple locations in different networks then below table shows what network ports must be enabled in firewall to allow domain traffic in the environment.

|  |  |  |
| --- | --- | --- |
| **Client Port(s)** | **Server Port** | **Service** |
| 1024-65535/TCP | 135/TCP | RPC Endpoint Mapper |
| 1024-65535/TCP | 1024-65535/TCP | RPC for LSA, SAM, NetLogon (\*) |
| 1024-65535/TCP/UDP | 389/TCP/UDP | LDAP |
| 1024-65535/TCP | 636/TCP | LDAP SSL |
| 1024-65535/TCP | 3268/TCP | LDAP GC |
| 1024-65535/TCP | 3269/TCP | LDAP GC SSL |
| **Record Name** | **Description** | **Description** |
| 1024-65535/TCP/UDP | 88/TCP/UDP | Kerberos |
| 1024-65535/TCP | 445/TCP | SMB |
| 1024-65535/TCP | 1024-65535/TCP | FRS RPC (\*) |

# **Non-Active Directory Roles and applications**

Fundamentally the function of Domain controllers is to manage user authentication and authorization on computers and applications in a domain and Active directory Domain services (ADDS) along with DNS role must be installed to promote any member server as domain controller in a domain. Other than ADDS and DNS no other roles or features should not be installed on domain controllers as a best practice or recommendation. Why because for example, if print or file services are running on domain controller, according to security compliance when domain controller upgrade is needed, it is quite challenging to address print/file server migration to other member server due to complexity in test and validation of those services post migration. So non-AD roles must not be running on domain controllers.

Part of the assessment job, it is important to document information about non-AD roles and non-domain applications that are installed on every domain controller in AD Forest/domain. Work with the customer and respective stakeholders to move out non-AD roles and applications from the domain controller to other member servers or appliances before performing domain controller upgrade to latest version of Windows server.

For example, in some scenarios you can find DHCP server running on Domain Controllers, based on the Customer’s standard operating procedures, if DHCP should be owned by network team, then work with network team to move the role to IPAM based appliance or else if the support is hold by Windows team, then migrate it to other member server which has latest operating system.

# **Domain Controller Upgrade Considerations**

What is domain controller upgrade? It is not suggestible to carry out in-place upgrade of domain controller, because most of the cases operating system experience issues post upgrade and it is a cumbersome task to troubleshoot and resolve those issues. So, it's recommended to migrate domain controllers to new servers instead of performing an in-place upgrade.

* 1. **Application Hardcoding**

Few of the applications in the environment can be hardcoded with the name or IP of a domain controller. Most of the cases IP address is being used for hardcoding, so when you get a new domain controller with new IP Address, then applications will lose domain authentication. Therefore, after demoting the old domain controller, it is advised to configure the new domain controller with the legacy domain controller's IP address.

**Note:** Section 4 has covered hardware platforms considerations.

* 1. **Retain IP Address of Legacy Domain controller – platform-based considerations.**

Considering the dependencies on application hardcoding of domain controller IP, when you are planning to swap IP address of new domain controller with legacy domain controller IP to retain it, you need to understand challenges of underlying platform on which domain controller is running.

* When domain controller is running on physical server, it’s a straightforward task to retain IP address by following operating system upgrade procedures on it.
* When domain controller is running on VMWare or Hyper-V platforms, IP address can be reconfigured on new domain controller at OS level without any issues.
* When domain controller is running on Azure platform, you are not supposed to configure or reconfigure IP address inside operating system, you can ask Azure administrators to reconfigure IP address on VM network adapter
* When domain controller is running on AWS platform, you cannot configure legacy domain controller IP address on new domain controller. Because primary IP address is assigned to EC2 instance during when it is created and will be unassigned when EC2 instance is terminated as per Amazon. So IP SWAP on AWS domain controllers cannot be possible. Only way is to retain IP Address of Legacy domain controller in AWS is that you need to terminate Legacy Domain controller instance in AWS and assign that IP to new domain controller instance. Refer <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#concepts-private-addresses> for more details.
  1. **Domain Controllers Function Levels**

The domain or forest capabilities of Active Directory Domain Services (AD DS) are determined by functional levels. They also specify which Windows Server versions can be installed on domain controllers inside a given forest or domain. On workstations and member servers that are connected to the domain or forest, functional levels do not, however, impact the operating systems that can be installed on them.

Identify current function levels of forest and domain and verify whether new server build is compatible with the current function levels. For example, if you have Windows 2008 R2 function level in the customer environment, it supports below versions of windows servers for domain controllers build.

* Windows Server 2022
* Windows Server 2019
* Windows Server 2016
* Windows Server 2012 R2
* Windows Server 2012
* Windows Server 2008 R2

Windows Server 2012 function level – Supported domain controllers Operating System

* Windows Server 2022
* Windows Server 2019
* Windows Server 2016
* Windows Server 2012 R2
* Windows Server 2012

Windows Server 2012 R2 function level – Supported domain controller operating system

* Windows Server 2022
* Windows Server 2019
* Windows Server 2016
* Windows Server 2012 R2

Windows Server 2016 function level – Supported domain controller operating system

* Windows Server 2022
* Windows Server 2019
* Windows Server 2016

Apart from supported Operating system, you need to understand what the new features are introduced by Microsoft with latest version of operating system.

**Windows Server 2016 forest functional level features**

All the features that are available at the Windows Server 2012 R2 forest functional level, and the following features, are available:

* Privileged access management (PAM) using Microsoft Identity Manager (MIM)

**Windows Server 2016 Domain functional level features**

All default Active Directory features, all features from the Windows Server 2012 R2 domain functional level, plus the following features:

* DCs can support automatic rolling of the NTLM and other password-based secrets on a user account configured to require PKI authentication. This configuration is also known as "Smart card required for interactive logon”.
* DCs can support allowing network NTLM when a user is restricted to specific domain-joined devices.
* Kerberos clients successfully authenticating with the PKInit Freshness Extension will get the fresh public key identity SID.
* For more information, see What's New in Kerberos Authentication and What's new in Credential Protection

**Windows Server 2012 R2 Forest functional level features**

All the features that are available at the Windows Server 2012 forest functional level, but no additional features.

**Windows Server 2012 R2 Domain functional level features**

All default Active Directory features, all features from the Windows Server 2012 domain functional level, plus the following features:

* DC-side protections for Protected Users. Protected Users authenticating to a Windows Server 2012 R2 domain can no longer:
* Authenticate with NTLM authentication
* Use DES or RC4 cipher suites in Kerberos pre-authentication
* Be delegated with unconstrained or constrained delegation
* Renew user tickets (TGTs) beyond the initial 4 hour lifetime
* Authentication Policies
* New forest-based Active Directory policies that can be applied to accounts in Windows Server 2012 R2 domains to control which hosts an account can sign-on from and apply access control conditions for authentication to services running as an account.
* Authentication Policy Silos
* New forest-based Active Directory object, which can create a relationship between user, managed service and computer, accounts to be used to classify accounts for authentication policies or for authentication isolation.

For more information about features of previous versions of operating systems refer <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels>

* 1. **NTP Settings on Domain Controllers**

Below is the Time services configuration on every domain controller. To mitigate any existing time sync issues between PDC and ADCs or if you want to reconfigure NTP on entire domain, run below commands in elevated command prompt on every domain controller

**STEP 1:**

On PDC, run the following commands to update the time source:

*net stop w32time*

*w32tm /unregister*

*w32tm /register*

*net start w32time*

*w32tm /config /manualpeerlist:pool.ntp.org,0x8 /syncfromflags:MANUAL /reliable:yes /update*

*net stop w32time*

*net start w32time*

**STEP 2:**

Run the following commands to confirm new settings:

*w32tm /query /source*

*w32tm /query /peers*

*w32tm /query /status*

*w32tm /query /configuration*

**STEP 3:**

Force sync with pool.ntp.org and confirm time updates:

*w32tm /resync /force*

*w32tm /stripchart /computer:pool.ntp.org /dataonly /samples:1*

**STEP 4**

Other DCs\Member servers should point to the PDC for time.

*net stop w32time*

*w32tm /unregister*

*w32tm /register*

*net start w32time*

*w32tm /config /syncfromflags:domhier /update*

*net stop w32time*

*net start w32time*

Time Source on PDC should be external NTP server and Time Source on ADCs should be PDC.

* 1. **FRS for domain replication (Windows 2008 Domain controllers)**

File replication service is used in Windows 2008 to perform replication between two or multiple domain controllers within a forest and domain environment. FRS is deprecated in Windows 2008 R2, but still it uses FRS to replicate data between domain controllers.

However Windows 2012 and later versions do not use FRS, they use DFS-R technology for domain controllers replication.

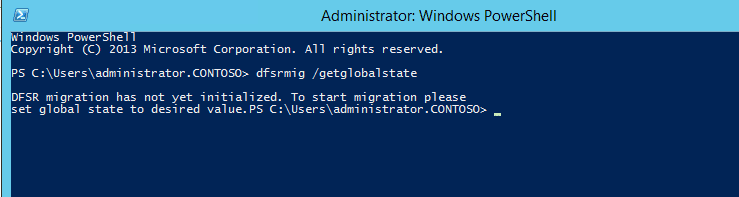
When you are trying to promote a domain controller which has latest version of windows operating system and you get error ***“verification of replica failed, the specified domain example.com is still using File Replication Service(FRS)”*** then you need to perform FRS to DFSR sysvol migration using below steps

You can verify if the system uses the FRS using dfsrmig /getglobalstate.

1) Log in to domain controller as Domain admin or Enterprise Admin

2) Launch powershell console and type dfsrmig /getglobalstate.

Below output confirms that it has not yet initiated the DFRS migration yet.



Before proceeding with any configuration changes, we suggest that you familiarize yourself with the migration stage.

Below are are four states that correspond with the four migration phases.

1) State 0 – Start

2) State 1 – Prepared

3) State 2 – Redirected

4) State 3 – Eliminated

**State 0 – Start**

With initiating this state, FRS will replicate the SYSVOL folder amongst the domain controllers. It is important to have a current copy of SYSVOL before begins the migration process to avoid any conflicts.

**State 1 – Prepared**

In this state, FRS continues replicating the SYSVOL folder while DFSR will replicate a copy of SYSVOL folder. It will be located in %SystemRoot%\SYSVOL\_DFRS by default. But this SYSVOL will not respond to any other domain controller service requests.

**State 2 – Redirected**

In this state, the DFSR copy of SYSVOL starts to respond for SYSVOL service requests. FRS will continue the replication of its own SYSVOL copy but will not involve with production SYSVOL replication.

**State 3 – Eliminated**

In this state, DFS Replication will continue its replication and servicing SYSVOL requests. Windows will delete original SYSVOL folder users by FRS replication and stop the FRS replication.

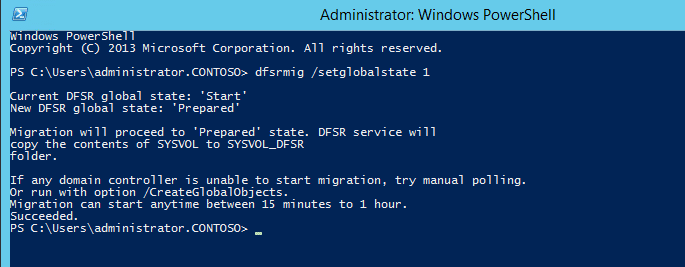
In order to migrate from FRS to DFSR it must to go from State 1 to State 3. Let’s look into the migration steps in more detail.

Prepared State

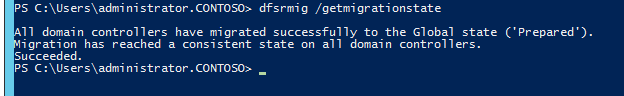
Log in to domain controller as Domain admin or Enterprise Admin

2. Launch PowerShell console

3. Type dfsrmig /setglobalstate 1 and press enter

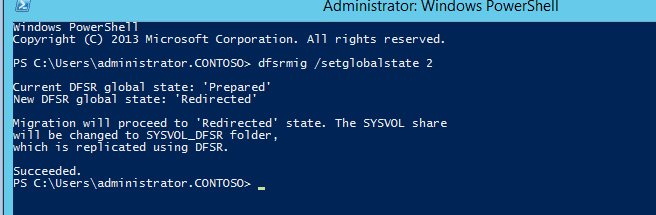


4. Type dfsrmig /getmigrationstate to confirm all domain controllers have reached the prepared state

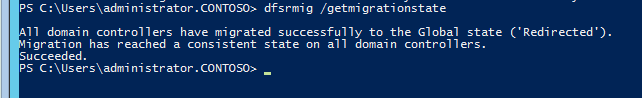


Log in to domain controller as Domain admin or Enterprise Admin

2. Launch PowerShell console

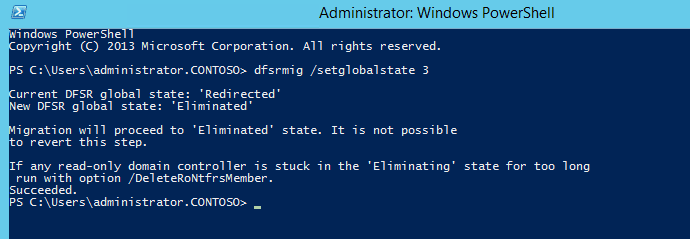
3. Type dfsrmig /setglobalstate2 and press enter

4. Type dfsrmig /getmigrationstate to confirm all domain controllers have reached redirected state

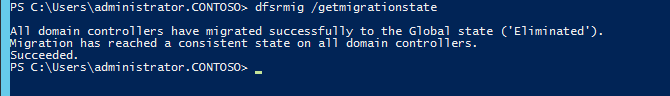


Log in to domain controller as Domain admin or Enterprise Admin

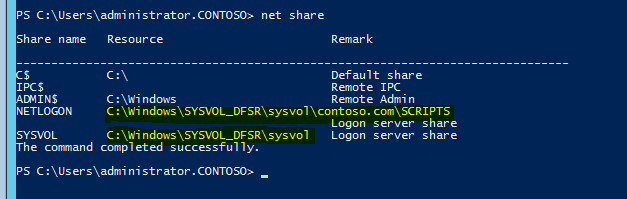
2. Launch powershell console

3. Type dfsrmig /setglobalstate 3and press enter

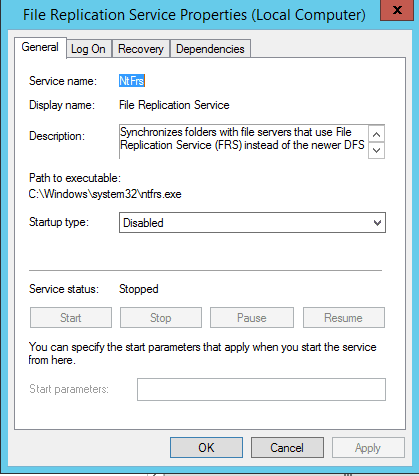
4. Type dfsrmig /getmigrationstate to confirm all domain controllers have reached eliminated state



This completes the migration process and to confirm the SYSVOL share, type net share command and press enter.



Also make sure in each domain controller FRS service is stopped and disabled.



* 1. **Domain Controller Upgrade checklist**

Ensure that you have appropriate checklist of below tasks before performing domain controller upgrade.

* Existing domain should be in healthy state (AD Site replication should not have any replication issues and all tests should be passed in every domain controller) – Refer Section 7 for more information to troubleshoot existing issues in the AD domain and domain controllers.
* Request build team to get a new server build with latest version of windows server for additional domain controller deployment.
* Get the new build from platform or windows team.
* Ensure that new build has latest operating system installed.
* Check with Windows or platform team that post build activities are completed on new build that includes new patches installed, Antivirus, monitoring and other necessary agents installed based on the Customer standards.
* Verify IP Address, Mask, Gateway, and DNS configuration (This is very important because wrong configuration impacts domain controller promotion negatively in the existing forest domain)
* Add the domain controller to the existing Active Directory domain as a domain member.
* Find information about existing domain sites and the initial replication method.
* Log in to the server with a privileged account (such as Schema Admin or Enterprise Admin).
* Install the AD DS role.
* Configure AD DS.
* Configure NTP settings post domain controller configuration (Refer Sec 2.4)
* Run DC diagnostics and replication tools to validate health of new additional domain controller.
* Review the logs to verify healthy AD DS installation and configuration.
* In case of any errors, perform necessary troubleshooting and apply the solutions to resolve them.
  1. **Domain Controller Demotion Checklist**
* Transfer any FSMO roles to a DC that’s going to remain online.
* Remove Active Directory Domain Services role from DC.
* Demote domain controller to a member server.
* Clean up references in DNS Server
* Remove server from Sites and Services
* Update static IP addresses that are pointing to decommissioned domain controller.
* Perform replication checks in forest/domain

# **Remediating Issues in the Forest/Domain**

When you experience any issues related to replication or DC diagnostics, post domain controller upgrade then you must verify DNS, network routing and networking ports before carrying out further steps to troubleshoot and resolve.

Errors I have experienced:

1. PDC information will not be shown on domain controller when you run “nltest /sc\_query:domainName” command

**Resolution :** Ensure that NTP configuration is correct and suggesting you to reconfigure NTP on PDC and other domain controllers to resolve the issue.

1. Repadmin /replsummary shows “The Target Principal Name is incorrect” or “Access Denied”.

**Resolution:**

1. Stop KDC service and disable.
2. Reboot server
3. Run below command.
4. netdom resetpwd /server:PDC /userd:domainname\Administrator /passwordd:$password
5. Reboot server
6. Start KDC service and force replication from Sites and Services
7. Repadmin /replsummary shows “The RPC server is unavailable”.

**Resolution:**

1. Verify DNS is working.
2. Verify network ports are not blocked by a firewall or third-party application listening on the required ports.
3. Bad NIC drivers
4. UDP fragmentation can cause replication errors that appear to have a source of RPC server is unavailable.
5. SMB signing mismatches between DCs.

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/replication-error-1722-rpc-server-unavailable>