

# Active Directory: migrating from 2003 to 2012 R2 enterprise multi-site single forest domain

## Table of Contents

[Prior to moving forward](#)

[Prerequisites](#)

[Evaluate existing environment](#)

[Determine plan of action](#)

[Deploy physical and virtual Windows 2012 R2 servers to sites](#)

[Promote Windows 2012 R2 Servers to Domain Controllers](#)

[Validate replication of Windows 2012 R2 servers](#)

[Migrate DNS using Powershell on all Windows hosts that have static DNS](#)

[Manually change static DNS](#)

[Migrate any existing services off of domain controllers](#)

[Move FSMO roles to Windows 2012 R2 server](#)

[Demote existing Windows 2003 Domain Controllers to member servers](#)

[Validate replication of Windows 2012 R2 servers](#)

[Raise Forest/Domain functional level](#)

[Validate replication](#)

[References:](#)

[Helpful Scripts](#)

## Prior to moving forward

### Prerequisites

- Have proper media and licensing for Windows 2012 R2
- A firm understanding of DNS
- A firm understanding of DCDiag

- A firm understanding of NTDSUTIL
- A good understanding of FSMO roles
- A good understanding of DCPromo and Active Directory Domain Services (ADDS)
- A good understanding of basic networking
- A basic understanding of PowerShell

## Evaluate existing environment

Things to take note of:

- DNS – servers, printers, workstations, AP, scanners, applications, phone systems and anything else that could be using static DNS will need to change.
- DHCP- Domain controllers with DHCP will need to have DHCP moved off to another server if possible off of a domain controller onto their own server depending on resources
- Database – database configurations using NTLM will need to change authentication methodologies.
- IIS or apache – websites using NTLM will need to change authentication methodologies.
- NTP – Time protocol services will need to be updated in some environments (VMware hosts)
- File & Print Sharing on a domain controller – files need to be migrated off of the domain controller to another resource and stored in a location that is suitable for file sharing, printers will need to be relocated to another source that is suitable for print sharing
- Linux / Apple Environments – make sure you take note of LDAP settings on Linux and/or Apple environments. These settings will likely need to be changed.
- Existing applications that use AD for authentication –web based or form based application that are using static names will need to be updated or changed best practice would dictate to use the domain name instead of a domain controller I.E.: use domain.local versus domaincontroller.domain.local

## Determine plan of action

- Check for any existing problems within Active Directory, services, and resources that require LDAP
- Run DCDiag to diagnose any issues with AD. DCDiag should be run against your domain controllers frequently to determine faults in replication, domain controller issues, lost connections between domain controllers and general health of your domain. I ran into a slew of problems with DNS not replicating, old tombstoned domain controllers, invalid site settings and poor replication between sites. Be sure to address EVERY single issue and get it fixed PRIOR to deploying your first Windows 2012 R2 domain controller. DCDiag can point you in the right direction and Technet will help you solve these issues. In the event of a failure you can use NTDSUtil a Dos command prompt to remove domain controllers that have been tombstoned if you are unable to remove them through the GUI.
- A script for DNS health check you can use this script to determine if there are any issues in DNS
  - <https://gallery.technet.microsoft.com/DNS-Health-Report-80fa9675>
- FSMO roles...
  - Check to see FSMO roles are intact. If they are not then this needs to be resolved ASAP. This can be done using NTDSUtil.
  - FSMO role description: <https://support.microsoft.com/en-us/kb/197132>
- Using NTDSUtil to seize the roles and transfer them to another domain controller
  - <https://support.microsoft.com/en-us/kb/255504>

Understand this process is a little convoluted and can be a pain in the ass but this has to be done. These roles are essential for every function of Active Directory and have to be on a good working domain controller.

- NTP Network Time Protocol is really important. It is used to keep everything “on time”. Replication relies on NTP, workstations rely on accurate NTP settings for updating Group Policy and some services. Make sure that if you have statically assigned NTP servers that are domain controllers that they are changed to the

Windows 2012 R2 Global Catalog servers. (Specifically in VMware hosts this setting will likely need to be changed.)

- Meet with development teams to discuss the migration from 2003 to 2012 R2
- Authentication in some applications may be using NTLM for authentication, NTLM is no longer supported in 2012 R2 for authentication, Kerberos is used. If applications are still using NTLM they will need to be updated or upgraded to meet this requirement.

## Deploy physical and virtual Windows 2012 R2 servers to sites

Without changing the existing domain and forest functional levels you can deploy new Windows 2012 R2 domain controllers into the existing environment. You will need to forest prep and domain prep your existing environment prior to deployment. This can be done by going to the installation media of Windows 2012 R2 and running a Forestprep & DomainPrep.

## Promote Windows 2012 R2 Servers to Domain Controllers

Once the forest and domain preps have been completed, deploy Active Directory Domain Services on your first Windows 2012 R2 domain controller. I would suggest making this a Global Catalog Server and having it in close proximity with any other Windows 2003 Global Catalog Server(s) you may have.

Deploying the first domain controller is not without its issues but there is a really good article:

<http://blogs.technet.com/b/askpfeplat/archive/2012/09/03/introducing-the-first-windows-server-2012-domain-controller.aspx> 

## Validate replication of Windows 2012 R2 servers

This is absolutely crucial. Using DCDiag validate replication between your 2003 and 2012 domain controllers. If there are problems they need to be corrected immediately. You do not want to move forward with your migration plan if you are having problems with your first Windows 2012 R2 domain controller deployment. If you have successfully deployed first Windows 2012 R2 domain controller proceed to deploy more at your other sites. Be sure to check replication between sites, replication between controllers, and change DNS on domain controllers. Key is to remember to change DNS on old controllers to point to new Global Catalog servers.

# Migrate DNS using Powershell on all Windows hosts that have static DNS

This is the easy part. On machines windows based machines 2003 and up you can run a fast and easy PowerShell script against a list and have DNS changed to the new domain controller. This will only work on Windows based machines. My suggestion is to run a scan against your existing subnets, with a WMI query for DNS Primary and Secondary. Most network scanning utilities will allow for custom WMI queries so doing this will save you a significant amount of leg work. Changing DNS does not require a reboot. It is an instant process and as long as the DNS IP address is correct you will be good to go.

## Manually change static DNS

There are some resources that will need to have DNS manually changed, like:

- Printers, scanners, access points, layer 3 switches, routers , firewalls, Linux machines, Apple machines, phone systems, DHCP (don't forget DNS changes in DHCP need to reflect new DNS servers!), IIS/Apache using NTLM,SQL databases, applications, NTP on VMware hosts

Don't just rely on what you know about your environment. Ask developers, network admins, server admins, managers and anyone else that has been in the environment longer than you.


## Migrate any existing services off of domain controllers

- Migrate File & Print Sharing & DHCP services to new servers
- Migrate any applications on domain controllers to new servers.

## Move FSMO roles to Windows 2012 R2 server

Once you have a good solid Windows 2012 R2 domain controller in place you want to move your FSMO roles to it. This is VERY important and is a required step prior to decommissioning any old Windows 2003 domain controllers out of your environment.

To move the roles from the GUI use the following information

- <https://support.microsoft.com/en-us/kb/255690> 

To move the roles using NTDSUtil

- <https://support.microsoft.com/en-us/kb/255504> 

Prior to decommissioning any servers you want to make sure that FSMO roles are moved to one of the new Windows 2012 R2 domain controllers

## Demote existing Windows 2003 Domain Controllers to member servers

Once you are confident that you have migrated your required services from the Windows 2003 servers to new servers you can proceed to decommission the old domain controllers.

DCPromo is used to promote and decommission a domain controller. You can use DCPromo on the Windows 2003 servers to demote them to domain member servers. Once the Windows 2003 servers are domain member servers you can remove any other services (like DNS). At this point if you are confident you can proceed to either remove these servers from your domain or shut them down as they are no longer needed. If you shut them down you can start them back up in the even that they are back online. I ran into an issue with a few devices that I missed static DNS on and had to enable DNS forwarding on Windows 2003 servers that still had DNS services but were no longer domain controllers. I just put a forward address on the windows 2003 server to point to the new 2012 R2 server and when I had time changed DNS on the device connecting. To see what was still connecting to the Windows 2003 DNS server I would run a log file in DNS for about 30 minutes. Once those log files were clean with NO DNS queries I would uninstall DNS from the Windows 2003 server. This was pretty convenient in remote locations with poor bandwidth, gave me a little time before migrations to complete DNS changes.

## Validate replication of Windows 2012 R2 servers

Anytime you make a change to Active Directory Domain Services it is HIGHLY recommended that you pay close attention to replication. Make sure that old domain controllers that have been removed have had their records clean up and that domain controllers are no longer replicating to them. Make sure DNS is working properly and that you have good DNS replication between sites and domain controllers. Active Directory Domain Services replicated every 10 – 15 minutes depending on site replication settings and bandwidth. (This can be changed in sites and services but is no longer recommended to change in a Windows 2012 R2 environment since Distributed File System (DFS) is now used for replication.

# Raise Forest/Domain functional level

Once you have meet with the developers, the final applications have been updated or upgraded you and everyone has signed off on raising the Forest and Domain functional level. Get it done. These changes will likely require you to reboot your domain controllers.

Use the following link to update the Forest Functional level

- <https://technet.microsoft.com/en-us/library/Cc730985.aspx>

Raise the domain functional level

- <https://msdn.microsoft.com/en-us/library/Cc753104.aspx>



This change can take a while depending on number of domain controllers, problems in your environment and bandwidth. I'd suggest raising the functional levels slowly from 2003 to 2008, 2008 to 2008 R2, 2008 R2 – 2012, and eventually from 2012 to 2012 R2 over the course of a few weeks depending upon the size of your environment and other restrictions.

## Validate replication






Like every change validate replication. Make sure that Active Directory Domain Services is in perfect health. Run DCDiag and generate reports. Make sure DNS is healthy and you are not having issues with applications, services and/or resources.

## References:

- Step by step Active Directory migration from Windows Server 2003 to Windows Server 2012: <http://blogs.technet.com/b/canitpro/archive/2014/04/02/step-by-step-active-directory-migration-from-windows-server-2003-to-windows-server-2012.aspx>
- Migrating from previous versions to Windows 2012 R2: <https://technet.microsoft.com/en-us/dn408633.aspx>
- Step by step adding a Windows 2012 domain controller to an existing Windows 2003 network: <http://blogs.technet.com/b/canitpro/archive/2013/05/05/step-by-step-adding-a-windows-server-2012-domain-controller-to-an-existing-windows-2003-network.aspx>
- Introducing the first Windows 2012 domain controller: <http://blogs.technet.com/b/askpfplat/archive/2012/09/03/introducing-the-first-windows-server-2012-domain-controller.aspx>
- Understanding Active Directory Functional Levels: [https://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=WS.10).aspx)
- Raise Forest Functional Level: <https://technet.microsoft.com/en-us/library/Cc730985.aspx>
- Raise Domain Functional Level: <https://msdn.microsoft.com/en-us/library/Cc753104.aspx>

- Moving FSMO roles with NTDSUtil: <https://support.microsoft.com/en-us/kb/255504> 
- Moving FSMO roles with GUI: <https://support.microsoft.com/en-us/kb/255690> 

# Helpful Scripts

- DNS Health Report:
    - <https://gallery.technet.microsoft.com/DNS-Health-Report-80fa9675> 
  - User Security Audit:
    - <https://gallery.technet.microsoft.com/User-Security-Audit-Report-a382b84d> 
  - Set DNS with PowerShell:
    - <http://blogs.technet.com/b/heyscriptingguy/archive/2014/08/30/powertip-use-powershell-to-set-primary-and-secondary-dns-server-addresses.aspx> 
    - <http://community.spiceworks.com/topic/405339-replace-static-dns-settings-with-wmi-and-powershell> 
  - Active Directory Health Check:
    - <https://gallery.technet.microsoft.com/scriptcenter/Active-Directory-Health-709336cd> 
-