Understanding Windows Server 2008 Active Directory Domain and Forest Functional Levels

In Windows Server 2003, functional levels were an extension of the older mixed/native mode concept introduced in Windows 2000. In Windows Server 2008 this was further extended to include new features and benefits, and are used to activate new Active Directory features after all the Domain Controllers (DCs) in the domain or forest are running Windows Server 2008 operating systems. Functional levels determine the features of Active Directory Domain Services (AD DS) that are enabled in a domain or forest.

When the first Windows Server 2008–based Domain Controller is deployed in a domain or forest, the domain or forest operates by default at the lowest functional level that is possible in that environment, meaning Windows 2000 Native Mode. This allows you to take advantage of the default Active Directory features while running versions of Windows earlier than Windows Server 2008. When you raise the functional level of a domain or forest, a set of advanced features becomes available.

After the domain functional level is raised, DCs that are running earlier operating systems cannot be introduced into the domain. For example, if you raise the domain functional level to Windows Server 2008, Domain Controllers that are running Windows Server 2003 cannot be added to that domain.

Unless you still have old NT 4.0 BDCs there's no reason for staying in Mixed Mode, and as you already know, Windows Server 2008 does not support NT 4.0 BDCs, so if you are still using them and planning to upgrade your Active Directory to Windows Server 2008, re-think your strategy.

As for Windows 2000 Native Mode, unless you still have Windows 2000 Domain Controllers, again, there's no reason for staying in that function level. However, if you still do, remember that Windows Server 2008 does only supports Windows 2000 SP4. Be sure to have SP4 on all your Windows 2000 DCs.

You can read my "What are the domain and forest function levels in a Windows Server 2003-based Active Directory?" article for more info about that.

Note: Network clients can authenticate or access resources in the domain or forest without being affected by the Windows Server 2003 or Windows Server 2008 domain or forest functional levels. These levels only affect the way that domain controllers interact with each other. However, be aware of the fact that regardless of the domain or function level, servers running Windows NT Server 4.0 are **NOT** supported by domain controllers that are running Windows Server 2008, meaning you MUST have additional DCs running Windows 2000/2003 to support older NT 4.0 servers.

For more information about Windows Server 2008 Active Directory requirements, please read my "Active Directory on Windows Server 2008 Requirements" article.

Read my "Raising Windows Server 2008 Active Directory Domain and Forest Functional Levels" article for information on how to actually raise the domain and forest function levels.

Domain Function Levels

To activate a new domain function level, all DCs in the domain must be running the right operating system. After this requirement is met, the administrator can raise the domain functional level. Here's a list of the available domain function levels available in Windows Server 2008:

Windows 2000 Native Mode

This is the default function level for new Windows Server 2008 Active Directory domains.

Supported Domain controllers – Windows 2000, Windows Server 2003, Windows Server 2008.

Features and benefits:

- **Group nesting** – Unlike Windows NT 4.0, allows placing of a group of one scope as a member of another group of the same scope.
- **Universal security groups** – Allows usage of Universal security type groups.
- **SidHistory** – Enables usage of SidHistory when migrating objects between domains.
- **Converting groups between security groups and distribution groups** – Unlike Windows NT 4.0, allows converting of a group type into another group type (with some limitations).

Windows Server 2003 Mode

To activate the new domain features, all domain controllers in the domain must be running Windows Server 2003. After this requirement is met, the administrator can raise the domain functional level to Windows Server 2003. Read my "Raise Domain Function Level in Windows Server 2003 Domains" article for more info about that.

Supported Domain controllers – Windows Server 2003, Windows Server 2008.

Features and benefits include all default Active Directory features, all features from the Windows 2000 native domain functional level, plus:

- **Universal group caching** – Windows Server 2003 functional level supports Universal group caching which eliminate the need for local global catalog server.
- **Domain Controller rename** – By using the NETDOM command.
- **Logon time stamp update** – The lastLogonTimestamp attribute will be updated with the last logon time of the user or computer. This attribute is replicated within the domain.

- **Multivalued attribute replication improvements** – Allows incremental membership changes, which in turn enables having more than 5000 members in a group and better replication capabilities.
- **Lingering objects (zombies) detection** – Windows Server 2003 has the ability to detect zombies, or lingering objects.
- **AD-integrated DNS zones in application partitions** – This allows storing of DNS data in AD application partition for more efficient replication.
- **Users and Computers containers can be redirected** – This allows the redirection of the default location of new users and computers (by using the REDIRUSR and REDIRCMP commands).
- **Support for selective authentication** – Makes it possible to specify the users and groups from a trusted forest who are allowed to authenticate to resource servers in a trusting forest.

Windows Server 2008 Mode

o activate the new domain features, all domain controllers in the domain must be running Windows Server 2008. After this requirement is met, the administrator can raise the domain functional level to Windows Server 2008.

> **Important**
>
> Raising the domain and forest functional levels to Windows Server 2008 is a nonreversible task and prohibits the addition of Windows 2000–based or Windows Server 2003–based Domain Controllers to the environment. Any existing Windows 2000–based or Windows Server 2003–based Domain Controllers in the environment will no longer function, and in fact, the upgrading wizard will not allow you to continue with the operation. Before raising functional levels to take advantage of advanced Windows Server 2008 features, ensure that you will never need to install domain controllers running Windows 2000-based or Windows Server 2003–based Domain Controllers in your environment.

Supported Domain controllers – Windows Server 2008.

Features and benefits include all default Active Directory features, all features from the Windows Server 2003 domain functional level, plus:

- **Fine-grained password policies** – Allows multiple password polices to be applied to different users in the same domain.
- **Read-Only Domain Controllers** – Allows implementation of domain controllers that only host read-only copy of NTDS database.
- **Advanced Encryption Services** – (AES 128 and 256) support for the Kerberos protocol.
- **Granular auditing** – Allows history of object changes in Active Directory.
- **Distributed File System Replication (DFSR)** – Allows SYSVOL to replicate using DFSR instead of older File Replication Service (FRS). It provides more robust and detailed replication of SYSVOL contents.
- **Last Interactive Logon Information** – Displays the time of the last successful interactive logon for a user, from what workstation, and the number of failed logon attempts since the last logon.

Forest function levels

Forest functionality activates features across all the domains in your forest. To activate a new forest function level, all the domain in the forest must be running the right operating system and be set to the right domain function level. After this requirement is met, the administrator can raise the forest functional level. Here's a list of the available forest function levels available in Windows Server 2008:

Windows 2000 forest function level

This is the default setting for new Windows Server 2008 Active Directory forests.

Supported Domain controllers in all domains in the forest – Windows 2000, Windows Server 2003, Windows Server 2008.

Windows Server 2003 forest function level

To activate new forest-wide features, all domain controllers in the forest must be running Windows Server 2003. Read my "Raise Forest Function Level in Windows Server 2003 Active Directory" article for more info about that.

Supported Domain controllers in all domains in the forest – Windows Server 2003, Windows Server 2008.

Features and benefits include all default Active Directory features, plus the following features:

- **Forest trust.**
- **Domain rename.**
- **Linked-value replication** – Changes in group membership to store and replicate values for individual members instead of replicating the entire membership as a single unit.
- **Deployment of an RODC.**
- **Intersite topology generator (ISTG) improvements** – Supports a more efficient ISTG algorithm allows support for extremely large numbers of sites.
- **The ability to create instances of the dynamicObject dynamic auxiliary class.**
- **The ability to convert an inetOrgPerson object instance into a User object instance, and the reverse.**
- **The ability to create instances of the new group types, called application basic groups and Lightweight Directory Access Protocol (LDAP) query groups, to support role-based authorization.**
- **Deactivation and redefinition of attributes and classes in the schema.**

Windows Server 2008 forest function level

To activate new forest-wide features, all domain controllers in the forest must be running Windows Server 2008. Read my "Raising Windows Server 2008 Active Directory Domain and Forest Functional Levels" article for more info about that.

Supported Domain controllers in all domains in the forest – Windows Server 2008.

Features and benefits include all of the features that are available at the Windows Server 2003 forest functional level, but **no additional features**. All domains that are subsequently added to the forest will operate at the Windows Server 2008 domain functional level by default.