Understanding Active Directory Domain Services (AD DS) Functional Levels

92 out of 99 rated this helpful - Rate this topic

Updated: May 28, 2014

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2

Functional levels determine the available Active Directory Domain Services (AD DS) domain or forest capabilities. They also determine which Windows Server operating systems you can run on domain controllers in the domain or forest. However, functional levels do not affect which operating systems you can run on workstations and member servers that are joined to the domain or forest.

When you deploy AD DS, set the domain and forest functional levels to the highest value that your environment can support. This way, you can use as many AD DS features as possible. For example, if you are sure that you will never add domain controllers that run Windows Server 2003 to the domain or forest, select the Windows Server 2008 functional level during the deployment process. However, if you might retain or add domain controllers that run Windows Server 2003, select the Windows Server 2003 functional level.

When you deploy a new forest, you are prompted to set the forest functional level and then set the domain functional level. You cannot set the domain functional level to a value that is lower than the forest functional level. For example, if you set the forest functional level to Windows Server 2008, you can set the domain functional level only to Windows Server 2008. In this case, the Windows 2000 native and Windows Server 2003 domain functional level values are not available. In addition, all domains that you subsequently add to that forest have the Windows Server 2008 domain functional level by default.

You can set the domain functional level to a value that is higher than the forest functional level. For example, if the forest functional level is Windows Server 2003, you can set the domain functional level to Windows Server 2003or higher.

The following sections describe the features that are available at the different functional levels.

Features that are available at domain functional levels

The following table shows the features that are available at each domain functional level.

Domain functional level	Available features	Supported domain controller operating systems
Windows 2000 native	All of the default AD DS features and the following directory features are available: • Universal groups for both distribution and security groups. • Group nesting • Group conversion, which allows conversion between security and distribution groups • Security identifier (SID) history **Note** In Windows Server 2008 R2, the Personal Virtual Desktop feature was introduced. It requires the Windows 2000 native domain functional level. To deploy personal virtual desktops, your schema for the Active Directory forest must be at least Windows Server 2008. To use the added functionality provided by the **Personal Virtual Desktop** tab in the **User Account Properties** dialog box in Active Directory Users and Computers, you must run Active Directory Users and Computers from a computer running Windows Server 2008 R2 or a computer running Windows 7 that has Remote Server Administration Tools (RSAT) installed.	• Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003 • Windows 2000
Windows Server 2003	All the default AD DS features, all the features that are available at the Windows 2000 native domain functional level, and the following features are available: • The domain management tool, Netdom.exe, which makes it possible for you to rename domain controllers • Logon time stamp updates The **lastLogonTimestamp** attribute is updated with the last logon time of the user or computer. This attribute is replicated within the domain. • The ability to set the **userPassword** attribute as the effective password on **inetOrgPerson** and user objects • The ability to redirect Users and Computers containers	• Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003

	By default, two well-known containers are provided for housing computer and user accounts, namely, cn=Computers,<domain root> and cn=Users,<domain root>. This feature allows the definition of a new, well-known location for these accounts. • The ability for Authorization Manager to store its authorization policies in AD DS • Constrained delegation Constrained delegation makes it possible for applications to take advantage of the secure delegation of user credentials by means of Kerberos-based authentication. You can restrict delegation to specific destination services only. • Selective authentication Selective authentication makes it is possible for you 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	All of the default AD DS features, all of the features from the Windows Server 2003 domain functional level, and the following features are available: • Distributed File System (DFS) replication support for the Windows Server 2003 System Volume (SYSVOL) DFS replication support provides more robust and detailed replication of SYSVOL contents. **Note** Beginning with Windows Server 2012 R2, File Replication Service (FRS) is deprecated. A new domain that is created on a domain controller that runs at least Windows Server 2012 R2 must be set to the Windows Server 2008 domain functional level or higher. • Domain-based DFS namespaces running in Windows	• Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008

Server 2008 Mode, which includes support for access-based enumeration and increased scalability. Domain-based namespaces in Windows Server 2008 mode also require the forest to use the Windows Server 2003 forest functional level. For more information, see Choose a Namespace Type (http://go.microsoft.com/fwlink/?LinkId=180400).

- Advanced Encryption Standard (AES 128 and AES 256) support for the Kerberos protocol. In order for TGTs to be issued using AES, the domain functional level must be Windows Server 2008 or higher and the domain password needs to be changed.

  Note

  Authentication errors may occur on a domain controller after the domain functional level is raised to Windows Server 2008 or higher if the domain controller has already replicated the DFL change but has not yet refreshed the krbtgt password. In this case, a restart of the KDC service on the domain controller will trigger an in-memory refresh of the new krbtgt password and resolve related authentication errors.

- For more information, see Kerberos Enhancements.

- Last Interactive Logon Information

  Last Interactive Logon Information displays the following information:

  - The total number of failed logon attempts at a domain-joined Windows Server 2008 server or a Windows Vista workstation

  - The total number of failed logon attempts after a successful logon to a Windows Server 2008 server or a Windows Vista workstation

  - The time of the last failed logon attempt at a Windows Server 2008 or a Windows Vista workstation

  - The time of the last successful logon attempt at a Windows Server 2008 server or a Windows Vista workstation

	For more information, see Active Directory Domain Services: Last Interactive Logon (http://go.microsoft.com/fwlink/?LinkId=180387). • Fine-grained password policies Fine-grained password policies make it possible for you to specify password and account lockout policies for users and global security groups in a domain. For more information, see Step-by-Step Guide for Fine-Grained Password and Account Lockout Policy Configuration (http://go.microsoft.com/fwlink/?LinkID=91477). • Personal Virtual Desktops To use the added functionality provided by the **Personal Virtual Desktop** tab in the **User Account Properties** dialog box in Active Directory Users and Computers, your AD DS schema must be extended for Windows Server 2008 R2 (schema object version = 47). For more information, see Deploying Personal Virtual Desktops by Using RemoteApp and Desktop Connection Step-by-Step Guide (http://go.microsoft.com/fwlink/?LinkId=183552).	
Windows Server 2008 R2	All default Active Directory features, all features from the Windows Server 2008 domain functional level, plus the following features: • Authentication mechanism assurance, which packages information about the type of logon method (smart card or user name/password) that is used to authenticate domain users inside each user's Kerberos token. When this feature is enabled in a network environment that has deployed a federated identity management infrastructure, such as Active Directory Federation Services (AD FS), the information in the token can then be extracted whenever a user attempts to access any claims-aware application that has been developed to determine authorization based on a user's logon method. • Automatic SPN management for services running on a particular computer under the context of a Managed Service Account when the name or DNS host name of	• Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2

	the machine account changes. For more information about Managed Service Accounts, see Service Accounts Step-by-Step Guide (http://go.microsoft.com/fwlink/?LinkId=180401).	
Windows Server 2012	The **KDC support for claims, compound authentication, and Kerberos armoring** KDC administrative template policy has two settings (**Always provide claims** and **Fail unarmored authentication requests**) that require Windows Server 2012 domain functional level. For more information, see What's New in Kerberos Authentication.	• Windows Server 2012 R2 • Windows Server 2012

Windows Server 2012 R2	• 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 which 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.
		• Windows Server 2012 R2

Features that are available at forest functional levels

The following table shows the features that are available at each forest functional level.

Forest functional level	Available features	Supported domain controllers
Windows 2000	All of the default AD DS features are available.	• Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003 • Windows 2000
Windows Server 2003	All of the default AD DS features, and the following features, are available: • Forest trust • Domain rename • Linked-value replication Linked-value replication makes it possible for you to change group membership to store and replicate values for individual members instead of replicating the entire membership as a single unit. Storing and replicating the values of individual members uses less network bandwidth and fewer processor cycles during replication, and prevents you from losing updates when you add or remove multiple members concurrently at different domain controllers. • The ability to deploy a read-only domain controller (RODC) • Improved Knowledge Consistency Checker (KCC) algorithms and scalability The intersite topology generator (ISTG) uses improved	• Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003

	algorithms that scale to support forests with a greater number of sites than AD DS can support at the Windows 2000 forest functional level. The improved ISTG election algorithm is a less-intrusive mechanism for choosing the ISTG at the Windows 2000 forest functional level. • The ability to create instances of the dynamic auxiliary class named **dynamicObject** in a domain directory partition • The ability to convert an **inetOrgPerson** object instance into a **User** object instance, and to complete the conversion in the opposite direction • The ability to create instances of new group types to support role-based authorization. These types are called application basic groups and LDAP query groups. • Deactivation and redefinition of attributes and classes in the schema. The following attributes can be reused: ldapDisplayName, schemaIdGuid, OID, and mapiID. • Domain-based DFS namespaces running in Windows Server 2008 Mode, which includes support for access-based enumeration and increased scalability. For more information, see Choose a Namespace Type (http://go.microsoft.com/fwlink/?LinkId=180400).	
Windows Server 2008	All of the features that are available at the Windows Server 2003 forest functional level, but no additional features are available. All domains that are subsequently added to the forest, however, operate at the Windows Server 2008 domain functional level by default.	• Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008
Windows Server	All of the features that are available at the Windows Server	• Windows Server 2012

2008 R2	2003 forest functional level, plus the following features: • Active Directory Recycle Bin, which provides the ability to restore deleted objects in their entirety while AD DS is running. All domains that are subsequently added to the forest will operate at the Windows Server 2008 R2 domain functional level by default. If you plan to include only domain controllers that run Windows Server 2008 R2 in the entire forest, you might choose this forest functional level for administrative convenience. If you do, you will never have to raise the domain functional level for each domain that you create in the forest.	R2 • Windows Server 2012 • Windows Server 2008 R2
Windows Server 2012	All of the features that are available at the Windows Server 2008 R2 forest functional level, but no additional features. All domains that are subsequently added to the forest will operate at the Windows Server 2012 domain functional level by default.	• Windows Server 2012 R2 • Windows Server 2012
Windows Server 2012 R2	All of the features that are available at the Windows Server 2012 forest functional level, but no additional features. All domains that are subsequently added to the forest will operate at the Windows Server 2012 R2 domain functional level by default.	• Windows Server 2012 R2

Guidelines for raising domain and forest functional levels

The following guidelines apply to raising the domain or forest functional levels:

- You must be a member of the Domain Admins group to raise the domain functional level.
- You must be a member of the Enterprise Admins group to raise the forest functional level.

- You can raise the domain functional level on the primary domain controller (PDC) emulator operations master only. The AD DS administrative tools that you use to raise the domain functional level (the Active Directory Domains and Trusts snap-in and the Active Directory Users and Computers snap-in) automatically target the PDC emulator when you raise the domain functional level.

- You can raise the forest functional level on the schema operations master only. Active Directory Domains and Trusts automatically targets the schema operations master when you raise the forest functional level.

- You can raise the functional level of a domain only if all domain controllers in the domain run the version or versions of Windows Server that the new functional level supports.

- You can raise the functional level of a forest only if all domain controllers in the forest run the version or versions of Windows Server that the new functional level supports.

- You cannot set the domain functional level to a value that is lower than the forest functional level, but you can set it to a value that is equal to or higher than the forest functional level.

- With versions of Windows Server that are earlier than Windows Server 2008 R2, you cannot roll back or lower a functional level under any circumstances. If you have to revert to a lower functional level with a version of Windows Server that is earlier than Windows Server 2008 R2, you must rebuild the domain or forest or restore it from a backup copy.

- After you set the domain functional level, you cannot roll back or lower the domain functional level except in the cases listed in the following table. The domain functional level can be lowered only by using Windows

PowerShell. For more information, see Set-ADDomainMode.

Current domain functional level	Current forest functional level	Rollback options
Windows Server 2012 R2	Windows Server 2012 R2	None unless you first lower forest functional level
Windows Server 2012 R2	Windows Server 2012	Windows Server 2012
Windows Server 2012 R2	Windows Server 2008 R2	Windows Server 2012 or Windows Server 2008 R2
Windows Server 2012 R2	Windows Server 2008	Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008
Windows Server 2012	Windows Server 2012	None unless you first lower forest functional level
Windows Server 2012	Windows Server 2008 R2	Windows Server 2008 R2
Windows Server 2012	Windows Server 2008	Windows Server 2008 R2 or Windows Server 2008
Windows Server 2008 R2	Windows Server 2008 R2	None unless you first lower forest functional level
Windows Server 2008 R2	Windows Server 2008	Windows Server 2008
Windows Server 2008 or lower	Windows Server 2008 or lower	None

- After you set the forest functional level, you cannot roll back or lower the forest functional level except in the cases listed in the following table. The forest functional level can be lowered only by using Windows PowerShell. For more information, see Set-ADForestMode. For more information about the Active Directory Recycle Bin, see What's New in AD DS: Active Directory Recycle Bin (http://go.microsoft.com/fwlink/?LinkId=141392).

Current forest functional level	Recycle Bin enabled?	Rollback options
Windows Server 2012 R2	Yes	Windows Server 2012 or Windows Server 2008 R2

Windows Server 2012 R2	No	Windows Server 2012, Windows Server 2008, or Windows Server 2008 R2
Windows Server 2012	Yes	Windows Server 2008 R2
Windows Server 2012	No	Windows Server 2008 R2 or Windows Server 2008
Windows Server 2008 R2	Yes	None
Windows Server 2008 R2	No	Windows Server 2008