Knowledge Base

How to raise domain and forest functional levels in Windows Server 2003

PSS ID Number: 322692

Article Last Modified on 10/13/2004

The information in this article applies to:

- Microsoft Windows Server 2003, 64-Bit Datacenter Edition
- Microsoft Windows Server 2003, 64-Bit Enterprise Edition
- Microsoft Windows Server 2003, Datacenter Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, Standard Edition

This article was previously published under Q322692

IN THIS TASK

SUMMARY

This article describes how to raise the domain and forest functional levels that are supported by Microsoft Windows Server 2003 domain controllers. Functional levels are an extension of the mixed/native mode concept introduced in Microsoft Windows 2000 to activate new Active Directory features after all the domain controllers in the domain or forest are running the Windows Server 2003 operating system. When a computer that is running Windows Server 2003 is installed and promoted to a domain controller, new Active Directory features are activated by the Windows Server 2003 operating system over its Windows 2000 counterparts. Additional Active Directory features are available when all domain controllers in a domain or forest are running Windows Server 2003 and the administrator activates the corresponding functional level in the domain or forest.

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.

To activate new forest-wide features, all domain controllers in the forest must be running Windows Server 2003, and the current forest functional level must be at Windows 2000 native or Windows Server 2003 domain level. After this requirement is met, the administrator can raise the domain functional level.

Note Network clients can authenticate or access resources in the domain or forest without being affected by the Windows Server 2003 domain or forest functional levels. These levels only affect the way that domain controllers interact with each other.

back to the top

Domain Functional Level

Domain functionality activates features that affect the whole domain and that domain only. The four domain functional levels, their corresponding features, and supported domain controllers are as follows:

Windows 2000 mixed (Default)

- Supported domain controllers: Microsoft Windows NT 4.0, Windows 2000, Windows Server 2003
- Activated features: local and global groups, global catalog support

Windows 2000 native

- Supported domain controllers: Windows 2000, Windows Server 2003
- Activated features: group nesting, universal groups, SidHistory, converting groups between security groups and distribution groups, you can raise domain levels by increasing the forest level settings

Windows Server 2003 interim

- Supported domain controllers: Windows NT 4.0, Windows Server 2003
- Supported features: There are no domain-wide features activated at this level. All domains in a forest are automatically raised to this level when the forest level increases to interim. This mode is only used when you upgrade domain controllers in Windows NT 4.0 domains to Windows Server 2003 domain controllers.

Windows Server 2003

- Supported domain controllers: Windows Server 2003
- Supported features: domain controller rename, logon timestamp attribute updated and replicated. User password support on the InetOrgPerson objectClass. Constrained delegation, you can redirect the Users and Computers containers.

Domains that are upgraded from Windows NT 4.0 or created by the promotion of a Windows Server 2003-based computer operate at the Windows 2000 mixed functional level. Windows 2000 domains maintain their current domain functional level when Windows 2000 domain controllers are upgraded to the Windows Server 2003 operating system. You can raise the domain functional level to either Windows 2000 native or Windows Server 2003.

After the domain functional level is raised, domain controllers that are running earlier operating systems cannot be introduced into the domain. For example, if you raise the domain functional level to Windows Server 2003, domain controllers that are running Windows 2000 Server cannot be added to that domain.

The following describes the domain functional level and the domain-wide features that are activated for that level. Note that with each successive level increase, the feature set of the previous level is included.

back to the top

Forest Functional Level

Forest functionality activates features across all the domains in your forest. Three forest functional levels, the corresponding features, and their supported domain controllers are listed below.

Windows 2000 (default)

- Supported domain controllers: Windows NT 4.0, Windows 2000, Windows Server 2003
- New features: Partial list includes universal group caching, application partitions, install from media, quotas, rapid global catalog demotion, Single Instance Store (SIS) for System Access Control Lists (SACL) in the Jet Database Engine, Improved topology generation event logging. No global catalog full sync when attributes are added to the PAS Windows Server 2003 domain controller assumes the Intersite Topology Generator (ISTG) role.

Windows Server 2003 interim

- Supported domain controllers: Windows NT 4.0, Windows Server 2003. See the "Upgrade from a Windows NT 4.0 Domain" section of this article.
- Activated features: Windows 2000 features plus Efficient Group Member Replication using Linked Value Replication, Improved Replication Topology Generation. ISTG Aliveness no longer replicated. Attributes added to the global catalog. ms-DS-Trust-Forest-Trust-Info. Trust-Direction, Trust-Attributes, Trust-Type, Trust-Partner, Security-Identifier, ms-DS-Entry-Time-To-Die, Message Queuing-Secured-Source, Message Queuing-Multicast-Address, Print-Memory, Print-Rate, Print-Rate-Unit

Windows Server 2003

- Supported domain controllers: Windows Server 2003
- Activated features: all features in Interim Level, Defunct schema objects, Cross Forest Trust, Domain Rename, Dynamic auxiliary classes, InetOrgPerson objectClass change, Application Groups, 15-second intrasite replication frequency for Windows Server 2003 domain controllers upgraded from Windows 2000

After the forest functional level is raised, domain controllers that are running earlier operating systems cannot be introduced into the forest. For example, if you raise forest functional levels to Windows Server 2003, domain controllers that are running Windows NT 4.0 or Windows 2000 Server cannot be added to the forest.

back to the top

Interim Level - Upgrade from a Windows NT 4.0 Domain

Windows Server 2003 Active Directory permits a special forest and domain functional level named Windows Server 2003 interim. This functional level is provided for upgrades of existing Windows NT 4.0 domains where one or more Windows NT 4.0 backup domain controllers (BDCs) must have to function after the upgrade. Windows 2000 domain controllers are not supported in this mode. Windows Server 2003 interim applies to the following scenarios:

- Domain upgrades from Windows NT 4.0 directly to Windows Server 2003.
- Windows NT 4.0 BDCs do not upgrade immediately.
- Windows NT 4.0 domains that contain groups with more than 5000 members not including the domain users group.
- There are no plans to implement Windows 2000 domain controllers in the forest at any time.

Windows Server 2003 interim provides two important enhancements while still permitting replication to Windows NT 4.0 BDCs:

1. Efficient replication of security groups, support for more than 5000 members per group.
2. Improved KCC inter-site topology generator algorithms.

Because of the efficiencies in group replication that is activated in the interim level, this is the recommended level for all Windows NT 4.0 upgrades. See the "Best Practices" section of this article for more details.

Setting Windows Server 2003 Interim Forest Functional Level

Windows Server 2003 interim can be activated in three different ways. The first two methods are highly recommended because security groups use linked value replication (LVR) after the Windows NT 4.0 domain's primary domain controller (PDC) has been upgraded to a Windows Server 2003 domain controller. The third option is sub-optimal because membership in security groups uses a single multi-valued attribute which may result in replication issues. The ways in which Windows Server 2003 interim can be activated are:

1. During the upgrade.

   The option is presented in Dcpromo installation wizard when you upgrade the PDC of a Windows NT 4.0 domain that serves as the first domain controller in the root domain of a new forest.
2. Before you upgrade the Windows NT 4.0 PDC of a Windows NT 4.0 as the first domain controller of a new domain in an existing forest by manually configuring the forest functional level by using Lightweight Directory Access Protocol (LDAP) tools.

   Child domains inherit the forest-wide functionality settings from the forest they are promoted into. Upgrading the PDC of a Windows NT 4.0 domain as a child domain in an existing Windows Server 2003 forest where interim forest functional levels had been configured by using the Ldp.exe file or the Adsiedit.msc file permits security groups to use linked value replication after the OS version upgrade.
3. After the upgrade by using LDAP tools.

   The last two options are used when you join an existing Windows Server 2003 forest during an upgrade. This is a common scenario when an “empty root” domain is in position. The upgraded domain is joined as a child of the empty root and inherits the domain setting from the forest.

back to the top

Raise the Domain Functional Level

CAUTION: Do not raise the domain functional level if you have, or will have, any Windows NT 4.0 or earlier domain controllers. As soon as the domain functional level is raised to Windows 2000 native or Windows Server 2003, it cannot be changed back to a Windows 2000 mixed domain.

1. Log on the PDC of the domain with domain administrator credentials.
2. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Domains and Trust**.
3. In the console tree, right-click the domain for which you want to raise functionality, and then click **Raise Domain Functional Level**.
4. Under **Select an available domain functional level**, do one of the following:

- ○ Click **Windows 2000 native**, and then click **Raise** to raise the domain functional level to Windows 2000 native.

  -or-
- ○ Click **Windows Server 2003**, and then click **Raise** to raise the domain functional level to Windows Server 2003.

Note You can also raise the domain functional level by right-clicking a domain that appears in the Active Directory Users and Computers MMC snap-in, and then clicking **Raise Domain Functional Level**. To raise the domain functional level, you must be a member of the Domain Administrators group.

The current domain functional level appears under **Current domain functional level** in the **Raise Domain Functional Level** dialog box. The level increase is performed on the PDC FSMO and requires the domain administrator.

back to the top

Raise the Forest Functional Level

CAUTION: Do not raise the forest functional level if you have, or will have, any domain controllers running Windows NT 4.0 or Windows 2000. As soon as the forest functional level is raised to Windows Server 2003, it cannot be changed back to the Windows 2000 forest functional level.

1. Log on to the PDC of the forest root domain with a user account that is a member of the Enterprise Administrators group.
2. Open Active Directory Domains and Trusts, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
3. In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Raise Forest Functional Level**.
4. Under **Select an available forest functional level**, click **Windows Server 2003**, and then click **Raise**.

   Note To raise the forest functional level, you must upgrade (or demote) all existing Windows 2000 domain controllers in your forest.

   If you cannot raise the forest functional level, you can click **Save As** in the **Raise Forest Functional Level** dialog box to save a log file that specifies which domain controllers in the forest still must be upgraded from Windows NT 4.0 or Windows 2000.

   If you receive a message that indicates you cannot raise the forest functional level, use the report generated by "Save As" to identify all domains and domain controllers that do not meet the requirements for the requested increase.

   The current forest functional level appears under **Current forest functional level** in the **Raise Forest Functional Level** dialog box. After the forest level is successfully increased and replicated to the PDCs in the domains, the PDCs for each domain automatically increase their domain level to the current forest level. The level increase is performed on the Schema FSMO and requires Enterprise Administrator credentials.

back to the top

View and Set Functional Levels Manually

LDAP tools such as Ldp.exe and Adsisdedit.msc can be used to view and modify the current domain and forest functional level settings. When you modify the attributes manually, it is best to target the FSMO authoritative for the increase as the change is actually written to the authoritative FSMO then replicated.

Forest Level Setting

The attribute is msDS-Behavior-Version on the CN=Partitions, CN=Configurations, DC=ForestRootDom, DC=tld object.

- Value of 0 or not set=mixed level forest
- Value of 1=Windows Server 2003 interim forest level
- Value of 2=Windows Server 2003 forest level

  Note When you increase the msDS-Behavior-Version attribute from 0 to 1 with ADSIEdit, you receive the following error message:
  Illegal modify operation. Some aspect of the modification is not permitted.

Click **OK** to continue. The attribute on the partitions container and the domain head are correctly increased. The error message is not reported by the Ldp.exe file. You can safely ignore the error message. To verify the level increase was successful, refresh the attribute list and check the current setting. This error message may also occur if you have already performed the level increase on the authoritative FSMO, but has not replicated to the local domain controller.

Domain Functional Level Setting

The attribute is msDS-Behavior-Version on the NC head root of each domain DC=Mydomain, DC=ForestRootDom, DC=tld object.

- Value of 0 or not set=mixed level domain
- Value of 1=Windows Server 2003 domain level
- Value of 2=Windows Server 2003 domain level

Mixed/Native Mode Setting

The attribute is ntMixedDomain on the NC head root of each domain DC=Mydomain, DC=ForestRootDom, DC=tld object.

- Value of 0=Native level domain
- Value of 1=Mixed level domain

Quickly View the Current Settings By Using the Ldp.exe File

1. Start the Ldp.exe file.
2. On the **Connection** menu, click **Connect**.
3. Specify the domain controller you want to query, or leave the space blank to connect to any domain controller.

After you connect, the RootDSE information for the domain controller appears. The forest, domain, and domain controllers are included. The following is an example of the Windows Server 2003 domain controller, the domain mode is Windows Server 2003 and the forest mode is Windows 2000.

- 1> domainFunctionality: 2=(DS_BEHAVIOR_WIN2003)
- 1> forestFunctionality: 0=(DS_BEHAVIOR_WIN2000)
- 1> domainControllerFunctionality: 2=(DS_BEHAVIOR_WIN2003)

  Note The domain controller functionality represents the highest possible functional level for this domain controller, not at the function level that the domain controller is operating.

back to the top

Best Practices

The following section discusses the best practices for increasing functional levels. The section is broken into two parts, "Preparation Tasks" discusses the work that you must do before the increase, and "Optimal Paths Increase" discusses the motivations and methods for different level increase scenarios.

Preparation Tasks Before the Level Increase

Inventory the forest for earlier versions of domain controllers. If an accurate server list is not available, follow these steps:

1. To discover mixed level domains, Windows 2000 domain controllers, or domain controllers with damaged or missing objects, use Active Directory domains and trusts mmc snap-in.
2. Click **Raise Forest Functionality**, and then click **Save As** to generate a detailed report.

   If none were found, the option to increase to Windows Server 2003 forest level is available from the "Available Forest Functional Levels" drop down list. When you try to raise the forest level, the domain controller objects in the configuration containers is searched for any domain controllers that do not have msds-behavior-version equal to two. These are assumed to be either Windows 2000 domain controllers or damaged Windows Server 2003 domain controller objects. If earlier version domain controllers or domain controllers that have damaged or missing computer objects were found, they are included in the report. The status of these domain controllers must be investigated and the domain controllers representation in Active Directory must be repaired or removed by using the Ntdsutil file.

For additional information, click the article number below to view the article in the Microsoft Knowledge Base:

216498 How To Remove Data in Active Directory After an Unsuccessful Domain Controller Demotion

To discover Windows NT 4.0 domain controllers, follow these steps:

1. From any Windows Server 2003-based domain controller, open Active Directory Users and Computers.
2. If the domain controller is not already connected to the appropriate domain, follow these steps to connect to the appropriate domain:
   a. Right-click the current domain object, and then click **Connect to domain**.
   b. In the **Domain** dialog box, type the DNS name of the domain that you want to connect to or click **Browse** to select the domain from the domain tree, and then click **OK**.
3. Right-click the domain object, and then click **Find**.
4. In the **Find** dialog box, click **Custom Search**.
5. Click the domain for which you want to change the functional level.
6. Click the **Advanced** tab.
7. In the **Enter LDAP** query box, type the following and leave no spaces between any characters: `(&(objectCategory=computer)(operatingSystem Version=4*)(userAccountControl:1.2.840.113556.1.4.803:=8192))` **Note** This query is not case sensitive.
8. Click **Find Now**.

   A list of the computers in the domain that are running Windows NT 4.0 and functioning as domain controllers appears.

A domain controller may appear in the list for any of the following reasons:

- The domain controller is running Windows NT 4.0 and must be upgraded.
- The domain controller has been upgraded to Windows Server 2003 but the change has not replicated to the target domain controller.
- The domain controller is no longer in service but the computer object of the domain controller has not been removed from the domain.

Before you can change the domain functional level to Windows Server 2003, you must physically locate any domain controller in the list, determine the current status of the domain controller, and then either upgrade or remove the domain controller as appropriate. Note that unlike the Windows 2000 domain controllers, the Windows NT 4.0 domain controllers do not block a level increase. However, replication to the Windows NT 4.0 domain controllers stop. When you try to increase to Windows Server 2003 forest level with domains in Windows 2000 mixed level is blocked. The lack of Windows NT 4.0 BDCs is implied by meeting the forest level requirement of all domains at Windows 2000 native level or later.

Verify that End to End replication is working in the forest. To do so, use the Windows Server 2003 version of Repadmin on Windows XP or a Windows Server 2003 member against Windows 2000 or Windows Server 2003 domain controllers:

- Repadmin/Replsum * /Sort:Delta[/Errorsonly] for initial inventory.
- Repadmin/Showrepl * /CSV>showrepl.csv. Import to Excel, and then use the Data->Autofilter to identify replication features.

  Use replication tools such as Repadmin and Replmon to verify forest wide replication is working successfully.

Verify the compatibility of all programs or services with Windows Server 2003 domain controllers and Windows Server 2003 forest mode. Use lab environment to thoroughly test production programs and services for compatibility issues. Contact vendors for confirmation of capability.

Prepare a back out plan that includes of one of the following:

- Disconnect at least two domain controllers from each domain in the forest.

  -or-
- Create a system state backup of at least two domain controllers from each domain in the forest.

Before the back out plan can be used, all domain controllers in the forest must be decommissioned before the recovery process. Note that level increases cannot be authoritatively restored. So all domain controllers that are replicated in the level increase must be decommissioned.
After all the previous domain controllers are decommissioned, bring up the disconnected domain controllers or restore the domain controllers from backup. Remove the metadata from all the other domain controllers, and then re-promote them. This is a non-trivial process and must be avoided.

back to the top

How to Optimally Configure Functional Levels

The next two sections discuss two different paths to get from Windows 2000 mixed level to Windows Server 2003 forest level. The third section provides detailed information about Windows NT 4.0 upgrades.

All Domains Increased to Native Mode, the Forest Increased to Windows Server 2003

Increase all domains to Windows 2000 native level. After this is completed, increase the functional level for the forest root domain to Windows Server 2003 forest level. When the forest level replicates to the PDCs for each domain in the forest, the domain level is automatically increased to Windows Server 2003 domain level. This method has the following advantages:

- The forest-wide level increase is only performed one time. You do not have to manually increase each domain in the forest to the Windows Server 2003 domain functional level.
- A check for Windows 2000 domain controllers is performed before the level increase. The increase is blocked until the domain controllers are removed or upgraded. A detailed report can be generated by listing the blocking domain controllers providing actionable data.
- A check for domains in Windows 2000 mixed or Windows Server 2003 interim level is performed. The increase is blocked until the domain levels are increased to at least Windows 2000 native. Interim level domains must be increased to Windows Server 2003 domain level. A detailed report can be generated by listing the blocking domains.

All Domains Increased to Windows Server 2003 Domain Level, and then Increase the Forest to Windows Server 2003 Forest Level

Increase each domain to Windows Server 2003 domain level. This method has the following advantages:

- Windows Server 2003 domain level features are activated before committing the forest to Windows Server 2003 forest level.
- Interoperability testing can be performed on a smaller scale without committing the forest to Windows Server 2003 forest level.

back to the top

Windows NT 4.0 Upgrades

For Windows NT 4.0 upgrades always use interim level during the upgrade of the PDC unless Windows 2000 domain controllers are introduced into the forest. When interim mode is used during the upgrade of the PDC, the existing large groups use LVR replication immediately, avoiding potential replication issued discussed earlier in this article. Use one of the following methods to get to interim level during the upgrade:

- Select interim level during Dcpromo. This option is only presented when the PDC is upgraded into a new forest.
- Set the forest level of an existing forest to interim, and then join the forest during the upgrade of the PDC. The upgraded domain inherits the forest setting.
- After all the Windows NT 4.0 BDCs are upgraded or removed, each domain must be transitioned to forest level and can be transitioned to Windows Server 2003 forest mode.

A reason to avoid using interim mode is if there are plans to implement Windows 2000 domain controllers after the upgrade, or any time in the future.

Special Consideration for Large Groups in Windows NT 4.0

In mature Windows NT 4.0 domains, security groups that contain far more than 5000 members may exist. In Windows NT 4.0, when a member of a security group changes, only the membership single change is replicated to the backup domain controllers. In Windows 2000, group memberships are linked attributes stored in a single multi-valued attribute of the group object. When a single change is made to the membership of a group, the whole group is replicated as a single unit. Because the group membership is replicated as a single unit, there is a potential for updates to group membership to be "lost" when different members are added or removed at the same time at different domain controllers. Additionally, the size of this single object may be more than the buffer used to commit an entry into the database. For more information, see the "Version Store Issues with Large Groups" section of this article. For these reasons, the recommended limit for group members is 5000.

The exception to the 5000 member rule is the Domain Users group. The Domain Users group uses a "computed" mechanism based on the "primary group ID" of the user to determine membership and does not typically store members as multi-valued linked attributes. If the primary group of the user is changed, their membership in the Domain Users group is written to the linked attribute for the group and is no longer calculated. This was true for Windows 2000 and has not changed for Windows Server 2003. If the administrator does not select the interim level for the upgrade domain, you must follow these steps before the upgrade:

1. Inventory all large groups and identify any groups over 5000, except the domain users group.
2. All groups that have more than 5000 members must be broken into smaller groups that do not have more than 5000 members.
3. Locate all Access Control Lists where the large groups were entered and add the small groups used to split up the membership.

Windows Server 2003 interim forest level relieves administrators from having to discover and reallocate global security groups with more than 5000 members.

Version Store Issues with Large Groups

Active Directory uses a single block of memory for committing large changes to the database referred to as the "version store". When a large change is committed to the database, for example, when a large group is replicated in, the attribute change must be able to fit into the version store. If the attribute does not fit, the change cannot be committed, and replication of the attribute is effectively blocked. When groups reach large numbers, with more than 5000 members, they are at risk of using up the version store. Windows Server 2003 introduces a new replication mechanism named LVR, which addresses this limitation. LVR is activated when the forest functional level is raised to Windows Server 2003 interim forest level or Windows Server 2003 forest level. In this level, LVR is used to replicate groups between Windows Server 2003 domain controllers. The earlier Net Logon replication mechanism is used to replicate to the down-level Windows NT 4.0 domain controllers.

back to the top

Additional query words: kbactivedirectory

Keywords: kbActiveDirectory kbHOWTOmaster KB322692
Technology: kbWinServ2003Data kbWinServ2003Data64bit kbWinServ2003Data64bitSearch kbWinServ2003DataSearch kbWinServ2003Ent kbWinServ2003Ent64bit kbWinServ2003Ent64bitSearch kbWinServ2003EntSearch kbWinServ2003Search kbWinServ2003St

Send feedback to Microsoft