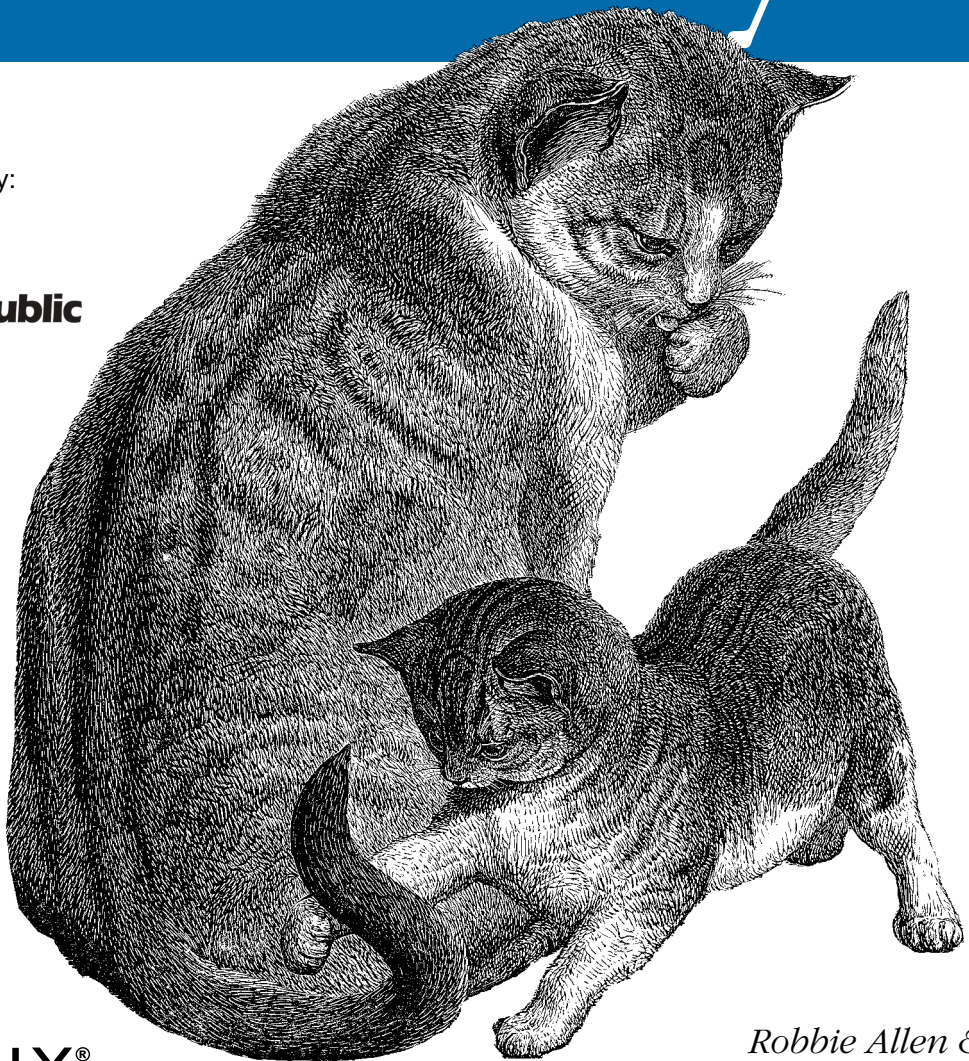


*Design and Deployment of
Microsoft's Active Directory*

2nd Edition
Covers Windows 2000 &
Windows .NET Server

Active Directory

Presented by:



O'REILLY®

*Robbie Allen &
Alistair G. Lowe-Norris*

Active Directory

SECOND EDITION

Active Directory

*Robbie Allen and
Alistair G. Lowe-Norris*

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

Upgrading to Windows Server 2003

The first version of Active Directory with Windows 2000 was surprisingly stable and robust. Microsoft does not have the best track record for initial releases of products, but they must be commended for Windows 2000 Active Directory in terms of its feature richness and reliability. That said, since Active Directory is such a complex and broad technology, there was still much room for improvement. There were some issues with scalability, such as the infamous 5,000-member limit with groups or the 300-site limit, which may have imposed artificial limitations on how you implemented Active Directory. Both of these issues have been resolved in Windows Server 2003. The default security setup with Windows 2000 Active Directory out-of-the-box was not as secure as it should have been. Signed LDAP traffic and other security enhancements have since been added into service packs, but they are provided by default with Windows Server 2003. Finally, manageability was another area that needed work in Active Directory, and in Windows Server 2003 numerous command-line utilities have been added along with some significant improvements to the AD Administrative snap-ins.

We have highlighted a few key areas where Active Directory has been improved in Windows Server 2003, and we'll describe more new features in the next section. If you already have a Windows 2000 Active Directory infrastructure deployed, your next big decision will be whether and when to upgrade to Windows Server 2003. Fortunately, the transition to Windows Server 2003 is evolutionary, not revolutionary, as with the migration from Windows NT to Active Directory. In fact, Microsoft's goal was to make the move to Windows Server 2003 as seamless as possible, and for the most part they have accomplished this. You can introduce Windows Server 2003 domain controllers at any rate you wish into your existing Active Directory environment; they are fully compatible with Windows 2000 domain controllers.

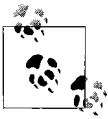
Before you can introduce Windows Server 2003 domain controllers, you must prepare the forest and domains with the ADPrep utility, which primes the forest for new features that will be available once you raise the functional level of the domain or forest. Functional levels are similar in nature to domain modes in Windows 2000 Active

Directory. They allow you to configure different levels of functionality that will be available in the domain or forest based on which operating systems are running on the domain controllers.

Before we cover the upgrade process to Windows Server 2003, we'll first discuss some of the major new features in Windows Server 2003 and some of the functionality differences with Windows 2000. Based on this information, you should be able to prioritize the importance of how quickly you should start migrating.

New Features in Windows Server 2003

While the release of Windows Server 2003 is viewed as evolutionary, there are quite a few new features that make the upgrade attractive.



By “feature” we mean new functionality that is not just a modification of the way it worked in Windows 2000. In this sense, a feature is something you have to use or implement explicitly. Functionality differences with Windows 2000 are covered in the next section.

We suggest you carefully review each of these features and rate them according to the following categories:

1. You would use the feature immediately.
2. You would use the feature eventually.
3. You would never use the feature or it is not important.

Rating each feature will help you determine how much you could benefit from the upgrade. The following is the list of new features, in no particular order:

Application partitions

You can create partitions that can replicate to any domain controller in the forest.

Concurrent LDAP binds

Concurrent LDAP binds do not generate a Kerberos ticket and security token and are therefore much faster than a simple LDAP bind.

Cross-forest trust

This is a transitive trust that allows all the domains in two different forests to trust each other via a single trust defined between two forest root domains.

Domain controller rename

The rename procedure for domain controllers requires a single reboot.

Domain rename

Domains can now be renamed, but not without significant impact to the user base (e.g. all member computers must be rebooted twice). For more

information, check out the following whitepaper: <http://www.microsoft.com/windowsserver2003/downloads/domainrename.msp>.

Dynamic auxiliary classes

There is now support for the standards-based implementation of dynamic auxiliary classes. Under Windows 2000, auxiliary classes are considered “static” because they are statically defined in the schema. With dynamic auxiliary classes, you can link one when creating an object without it being defined in the schema as an auxiliary class for the object’s objectClass.

Dynamic objects

Traditionally, objects are stored in Active Directory until they are explicitly deleted. With dynamic objects, you can create objects that have a time to live (TTL) value that dictates when they will be automatically deleted unless refreshed.

Install from media

A much-needed feature allows replica domain controllers to be promoted into a forest using a backup from another domain controller. This can greatly decrease the amount of time it takes to promote domain controllers in large domains.

MMC and CLI enhancements

The Active Directory Users and Computers (ADUC) tool has been enhanced to allow multiselect of objects; other tools such as *repadmin* and *netdom* have new options.

New DS CLI tools

A new set of CLI tools provides greater flexibility with managing Active Directory from a commandline. These tools include *dsadd*, *dsmod*, *dsrcm*, *dsget* and *dsquery*.

New GPO settings

Over 100 new GPO settings have been added, providing greater flexibility in managing Active Directory clients.

GPO RSoP

Resultant Set of Policy (RSoP) has been built into ADUC and can be fully utilized with the Group Policy Management Console (GPMC). RSoP allows administrators to determine what settings of GPOs will be applied to end users and computers.

TLS support

With Windows 2000, only SSL was supported to encrypt traffic over the wire. TLS, the latest standards-based approach for encrypting LDAP traffic, is now also supported.

Quotas

In Windows 2000, if users had access to create objects, they could create as many as they wanted, and there was no way to limit it. Quotas allow you to

define how many objects a user or group of users can create. Quotas can also dictate how many objects of a certain objectClass can be created.

Query based groups

Used for role-based authorization, the new Authorization Manager allows you to create flexible groups based on information stored with users (e.g., department).

Redirect users and computers

You can redirect the default location to store new users and computers with the *redirusr* and *redircmp* commands, respectively.

Schema redefine

You can defunct and then redefine attributes and classes in the schema.

Universal Group Caching

You can eliminate the requirement to have a global catalog server present during login by enabling Universal Group Caching. This is enabled at the site level and applies to any clients that log on to domain controllers in the site.

Last logon timestamp attribute

A classic problem in a NOS environment is trying to determine the last time a user or computer logged in. The new lastLogonTimestamp attribute is replicated, which means you can use a single query to find all users or computers that have not logged in within a certain period of time.

WMI filtering of GPOs

In addition to the OU, site, domain, and security group criteria that can be used to filter GPOs, you can now use WMI information on a client's machine to determine if a GPO should be applied.

WMI providers for trust and replication monitoring

These new WMI providers provide the ability to query and monitor the health of trusts and replication programmatically.

If you find that you would immediately use more than four or five features or eventually use four or five of them, the benefit may be great enough to warrant a near-term move to Windows Server 2003. If you don't find that you'll take advantage of many of these new features, take a look at the next section to see if you would benefit from any of the functionality differences with Windows 2000.

Differences With Windows 2000

Even though Active Directory was scalable enough to meet the needs of most organizations, there were some improvements to be made after several years of real-world deployment experience. Many of the functionality differences with Windows 2000 are the direct result of feedback from AD administrators.

As with the new features, we suggest you carefully review each of the differences and rate them according to the following categories:

1. It would positively affect my environment to a large degree.
2. It would positively affect my environment to a small degree.
3. It would negatively affect my environment.

The vast majority of differences are actually improvements that translate into something positive for you, but in some situations, such as with the security-related changes, the impact may cause you additional work initially.

Single instance store

Unique security descriptors are stored once no matter how many times they are used as opposed to being stored separately for each instance. This alone can save upwards of 20%–40% of the space in your DIT after upgrading. Note that an offline defragmentation will have to be performed to reclaim the disk space.

Account Lockout enhancements

Several bugs have been fixed which erroneously caused user lockouts in Windows 2000. A new Active Directory Users and Computers property page called Additional Account Info and the *lockoutstatus.exe* utility are great troubleshooting tools for diagnosing lockout problems.

Improved event log messages

There are several new event log messages that will aid in troubleshooting replication, DNS, FRS, etc.

Link value replication (LVR)

Replication in Active Directory is done at the attribute level. That is, when an attribute is modified, the whole attribute is replicated. This was problematic for some attributes, such as the member attribute on group objects, which could only store roughly 5,000 members. LVR replication means that certain attributes, such as member, will only replicate the changes within the attribute and not the contents of the whole attribute whenever it is updated.

Intrasite replication frequency changed to 15 seconds

The previous default was 5 minutes, which has now been changed to 15 seconds.

No global catalog sync for PAS addition

With Windows Server 2003, whenever an attribute is added to the Partial Attribute Set (PAS), a global catalog sync is no longer performed as it was with Windows 2000. This was especially painful to administrators of large, globally dispersed Windows 2000 domains.

Signed LDAP traffic

Instead of sending LDAP traffic, including usernames and passwords, over the wire in plain text with tools such as ADUC and ADSI Edit, the traffic is signed and therefore encrypted.

ISTG and KCC scalability improvements

The algorithms used to generate the intersite connections have been greatly improved to the point where the previous limit of 300 to 400 sites has been raised to support roughly 3,000–5,000 sites.

Faster global catalog removal

With Windows 2000, whenever you disabled the global catalog on a DC, the global catalog removal process could only remove 500 objects every 15 minutes. This has been changed so that the process is much quicker.

Distributed Link Tracking (DLT) service stopped by default

The DLT service can be the source of thousands if not millions of linkTrackO-MTEntry objects that are nestled within the System container of a domain. By default, the DLT service is disabled on Windows Server 2003 domain controllers.

Changes with Pre-Windows 2000 Compatible Access

To enhance security, the Everyone security principal no longer means all unauthenticated and authenticated users. It instead represents only authenticated users. To grant the equivalent of anonymous access in Windows Server 2003, the Anonymous Logon account should be added to the Pre-Windows 2000 Compatible Access group.

If you find that more than two or three of these would benefit your environment significantly, and fewer than one or two would have a negative affect, that is another good indication that an upgrade to Windows Server 2003 would benefit you enough to start in the near-term. This is by no means a hard-and-fast rule, since some features or differences may be more important than others. For example, if you have over 300 or 400 sites with domain controllers, the improvements in the KCC could potentially help you out significantly. Likewise, if you see the need to add attributes to the partial attribute set in the future, and you have large geographically disperse global catalog servers, then the no global catalog sync behavior could save you some long weekends babysitting replication. You may view other features, such as the MMC enhancements, as benefit, but not to the same degree as the other two just described. You'll have to weigh the priorities of each when you are considering them.

Functional Levels Explained

Now that you are sufficiently excited about the new features with Active Directory and improvements since Windows 2000, we will now cover how you can actually enable these features in Windows Server 2003. If you've already deployed Windows 2000 Active Directory, you are most certainly familiar with the domain mode concept. With Windows 2000 Active Directory, you had mixed- and native-mode domains. Domain mode simply dictated what operating systems were allowed to run on the domain controllers and nothing more. New features were enabled with the

move to native mode, including universal groups and group nesting to name a couple. Think of functional levels like domain modes, but taken a step further.

Windows Server 2003 functional levels are very similar to Windows 2000 domain modes from the standpoint that they dictate what operating systems can run on domain controllers, and they can only be increased or raised and never reversed. One common misunderstanding with domain modes, which hopefully will not be carried over to functional levels, is that they have virtually no impact on clients and what operating systems your clients run. For example, you can have Windows 9x clients in mixed- or native-mode Windows 2000 domains and also in domains that are at the Windows 2000 or Windows Server 2003 domain functional level.



For information about which operating systems are allowed at the various functional levels, check out the “Windows Server 2003 Functional Levels” section in Chapter 2.

An important difference with functional levels is that they apply both to domains and at the forest level. The reason for this is that some features of Windows Server 2003 Active Directory require either that all the domain controllers in a domain are running Windows Server 2003 or that all the domain controllers in the entire forest are running Windows Server 2003.

To illustrate why this is necessary, let’s look at two examples. First, let’s look at the new “Last logon timestamp attribute” feature. With this feature, a new attribute called `lastLogonTimestamp` is populated when a user or computer logs on to a domain, and it is replicated to all the domain controllers in a domain. This attribute provides an easier way to identify whether a user or computer has logged on recently than using the `lastLogon` attribute, which is not replicated and therefore must be queried on every domain controller in the domain. For `lastLogonTimestamp` to be of use, all domain controllers in the domain need to know to update it when they receive a logon request from a user or computer. Domain controllers from other domains only need to worry about the objects within their domain, so for this reason this feature has a domain scope. Windows 2000 domain controllers do not know about `lastLogonTimestamp` and do not update it. Therefore, for that attribute to be truly useful, all domain controllers in the domain should be running Windows Server 2003. All the domain controllers must know that all the other domain controllers are running Windows Server 2003, and they can do this by querying the functional level for the domain. Once they discover the domain is at a certain functional level, they start utilizing features specific to that function level.

Likewise, there are times when all domain controllers in the forest must be running Windows Server 2003 before a certain feature can be used. A good example is with the replication improvements. If some of the ISTGs were using the old site topology algorithms and others were using the new ones, you could have replication chaos. All domain controllers in the forest need to be running Windows Server 2003 before

the new algorithms are enabled. Until then, they will revert to the Windows 2000 algorithms.

How to Raise the Functional Level

To raise the functional level of a domain or forest, you can use the Active Directory Domains and Trusts MMC snap-in. To raise the functional level of a domain, open the snap-in, browse to the domain you want to raise, right-click on it in the left pane, and select “Raise Domain Functional Level...”. You will then see a screen similar to that in Figure 14-1.

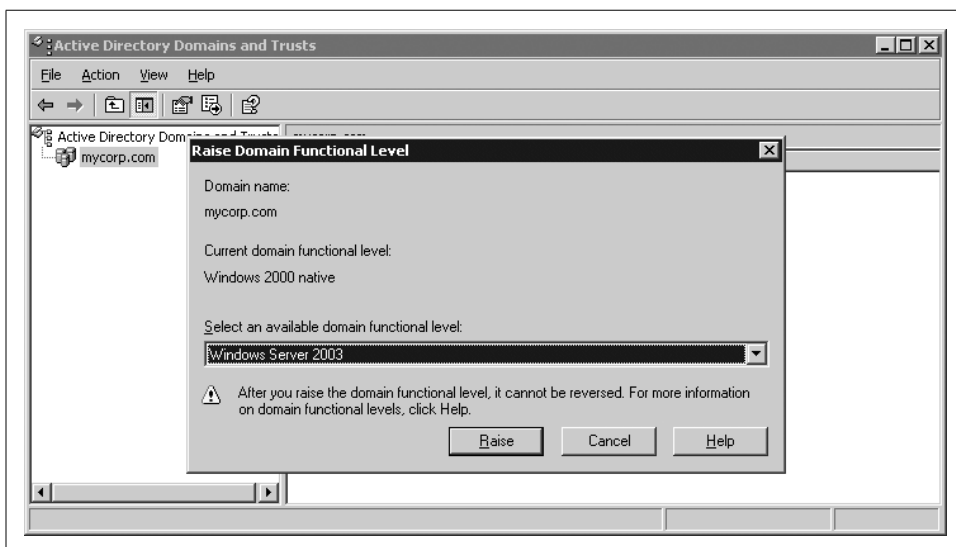


Figure 14-1. Raising the domain functional level

Select the new functional level and click the Raise button. You will then get a confirmation that it was successful or an error stating why it couldn't be raised. Figure 14-2 shows the message returned after successfully raising the functional level. Follow the same procedure to raise the functional level of a forest, but right-click on “Active Directory Domains and Trusts” in the left pane and select “Raise Forest Functional Level...”.

You can determine the functional level of a domain or forest two other ways. First, you can look at the msDS-Behavior-Version attribute on the Domain Naming Context (e.g., dc=mycorp,dc=com) for domains or the Partitions container in the Configuration Naming Context (e.g., cn=partitions,cn=configuration,dc=mycorp,dc=com) for the forest. A value of 0 indicates Windows 2000 functional level, 1 indicates Windows Interim functional level, and 2 indicates Windows Server 2003 functional level.

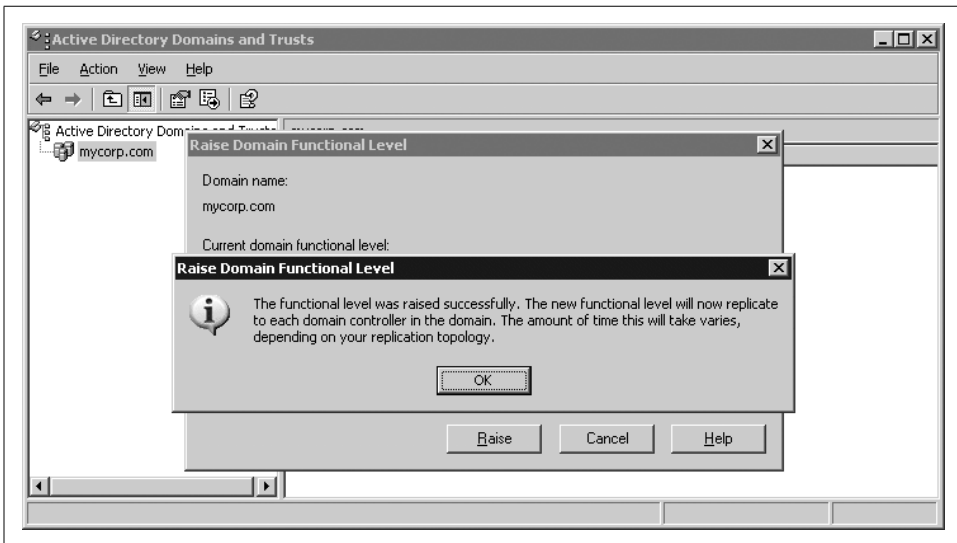


Figure 14-2. Result raising the domain functional level

Alternatively, you can view this information by simply looking at the RootDSE for a domain controller. On Windows Server 2003 domain controllers, the RootDSE contains two new attributes that describe the current functional level:

domainFunctionality

This value mirrors the msDS-Behavior-Version value on the Domain Naming Context.

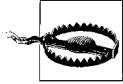
forestFunctionality

This value mirrors the msDS-Behavior-Version value on the Partitions container.

Preparing for ADPrep

Before you can start enabling functional levels, you have to go through the process of upgrading your existing infrastructure to Windows Server 2003. The first step before you can promote your first Windows Server 2003 domain controller is to prepare the forest with the ADPrep utility.

If you've installed Exchange 2000 into your Active Directory forest, you are undoubtedly familiar with the Exchange `setup.exe /forestprep` and `/domainprep` switches. These switches are run independently from the Exchange server install to allow Active Directory administrators to take care of the AD-related tasks necessary to support Exchange. The Exchange `/forestprep` command extends the schema and adds some objects in the Configuration Naming Context. The Exchange `/domainprep` command adds objects within the Domain Naming Context of the domain it is being run on and sets some ACLs. The ADPrep command follows the same logic and performs similar tasks to prepare for the upgrade to Windows Server 2003.



Microsoft recommends that you have at least Service Pack (SP) 2 installed on your domain controllers before running ADPrep. SP 2 fixed a critical internal AD bug, which can manifest itself when extending the schema. There were also some fixes to improve the replication delay that can be seen when indexing attributes. If you plan on supporting a mixed Windows 2000 and Windows Server 2003 environment for an extended period of time, Microsoft recommends that you have SP 3 on your Windows 2000 domain controllers.

For more information on the Microsoft recommendations, check out Microsoft Knowledge Base Article 331161 from <http://support.microsoft.com>.

The ADPrep command can be found in the `\i386` directory on the Windows Server 2003 CD. The ADPrep command depends on several files in that directory so it cannot simply be copied out and put on a floppy or CD by itself. To run the ForestPrep, you would execute the following:

```
X:\i386\adprep /forestprep
```

where *X*: is a CD drive or mapped drive to a network share containing the Windows Server 2003 CD. Similarly, to run DomainPrep you would execute the following:

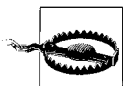
```
X:\i386\adprep /domainprep
```

You can view detailed output of the ADPrep command by looking at the log files in the `%SystemRoot%\system32\debug\adprep\logs` directory. Each time ADPrep is executed, a new log file is generated that contains the actions taken during that particular invocation. The log files are named based on the time and date ADPrep was run.

Now we will review what ForestPrep and DomainPrep do.

ForestPrep

The ADPrep `/forestprep` command extends the schema with quite a few new classes and attributes. These new schema objects are necessary for the new features supported by Windows Server 2003. You can view the schema extensions by looking at the `.ldf` files in the `\i386` directory on the Windows Server 2003 CD. These files contain LDIF entries for adding and modifying new and existing classes and attributes.



Microsoft warns against manually extending the schema with the ADPrep LDIF files. You should instead let ADPrep do it for you.

ForestPrep hardens some default security descriptors and modifies some of the ACLs on the containers in the Configuration NC. New displaySpecifier objects are added and some existing ones modified to support new features within the Active Directory Administrative snap-ins. A NTDS Quotas container is added at the root of the

Configuration container. This is a new container that hosts the quota objects that dictate how many objects a user or group of users can add within a container or OU.

One of the clever aspects of ADPrep is that it stores its progress in Active Directory. This is very neat because it can gracefully recover from failures halfway through execution. It also provides a quick way to determine whether all of the necessary operations have completed and whether ADPrep was successful. Another benefit of storing the operations in Active Directory is in case you encounter problems and need to call Microsoft Product Support Services (PSS). You can look at this container and list out all of the operations that have been successful. PSS would then be able to look up which operation is failing.

A ForestUpdates container is created directly under the Configuration container. Within the ForestUpdates container are two other containers, one called Operations and the other called Windows2003Update. The Operations container contains additional containers, each one representing a certain task that ADPrep completed. For example, one operation might be to create new displaySpecifier objects. The operation container names are GUIDs, and the objects themselves do not contain any information that would be of interest. There should be a total of 36 of these operation containers after ForestPrep completes.

The other object within the ForestUpdates container is called Windows2003Update. This object is created after ADPrep finishes. If that object exists, it signifies that ADPrep completed ForestPrep successfully. If you are interested to find out when ForestPrep completed in a forest, simply look at the whenCreated attribute on the Windows2003Update object. Figure 14-3 shows what these containers look like with the ADSI Edit snap-in from the Windows Support Tools.

You only need to execute ForestPrep once. You can run it multiple times, but due to the fact that it keeps track of its progress in Active Directory under the ForestUpdates container, it will only do something if it determines that an operation did not complete previously.

Since the schema is extended and objects are added in several places in the Configuration NC, the user running ForestPrep must be a member of both the Schema Admins and Enterprise Admins groups. In addition, you should run the command directly on the Schema Master for the forest. Importing the schema extensions is fairly resource-intensive, which is why it is necessary to run it from the Schema Master. Also, if you have large domains containing a lot of objects, ForestPrep may take a while to complete. ForestPrep indexes several attributes, which requires a lot of processing while it updates the AD database.

DomainPrep

Before you can run ADPrep /domainprep, you must be sure that the updates from ForestPrep have replicated to all domain controllers in the forest. DomainPrep must

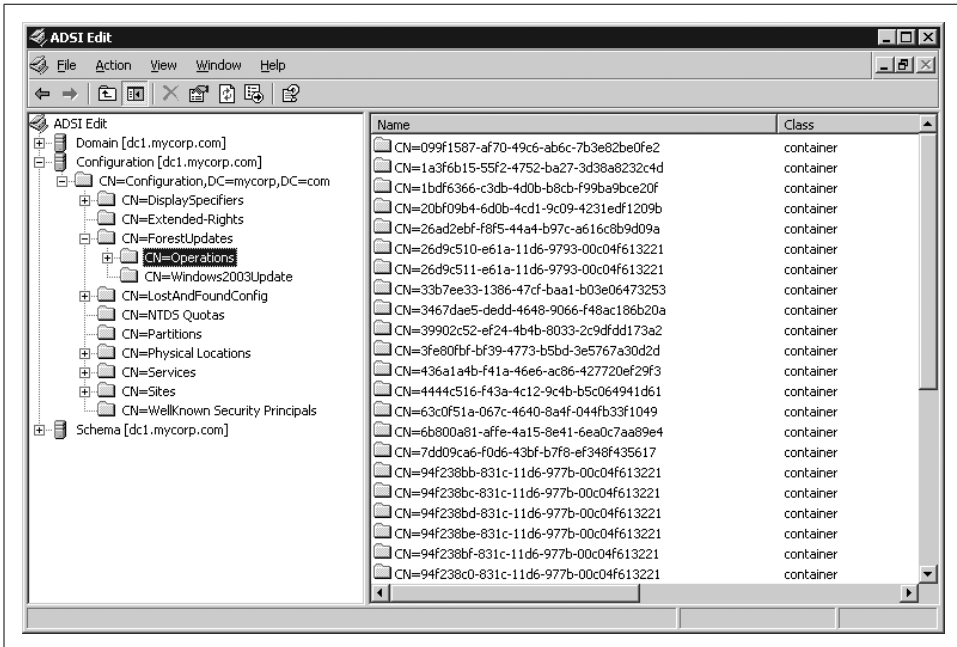


Figure 14-3. ADPrep forest update operations

be run on the Infrastructure Master of a domain and under the credentials of someone in the Domain Admins group. If you try to run DomainPrep before ForestPrep has been run or before it has replicated all its changes out, you will get an error message. Again, if you are unsure about the error, check the ADPrep logs in the `%SystemRoot%\system32\debug\adprep\logs` directory for more information.

DomainPrep creates new containers and objects, modifies ACLs on some objects, and changes the meaning of the Everyone security principal.

Unlike the ForestPrep command, which was fairly resource-intensive, DomainPrep completes quickly. The changes in comparison to ForestPrep are relatively minor. Two new top-level containers are created, one called NTDS Quotas, just like what ForestPrep added in the Configuration container, and another container called Program Data. This is intended to be a starting point for applications to store their data instead of each vendor coming up with their own top-level OU structure.

Just like with ForestPrep, DomainPrep stores the status of its completion in Active Directory. Under the System container, a DomainUpdates container is created. Within that container, two other containers are created, called DomainUpdates and Windows2003Update. The same principles apply here as did for ForestPrep. Each of the operations that DomainPrep performs is stored as an individual object within the Operations container. For DomainPrep there are 52 operations. After all the operations complete, the Windows2003Update object is written, which indicates Domain-

Prep has completed. Figure 14-4 shows an example of what this container structure looks like using ADSI Edit.

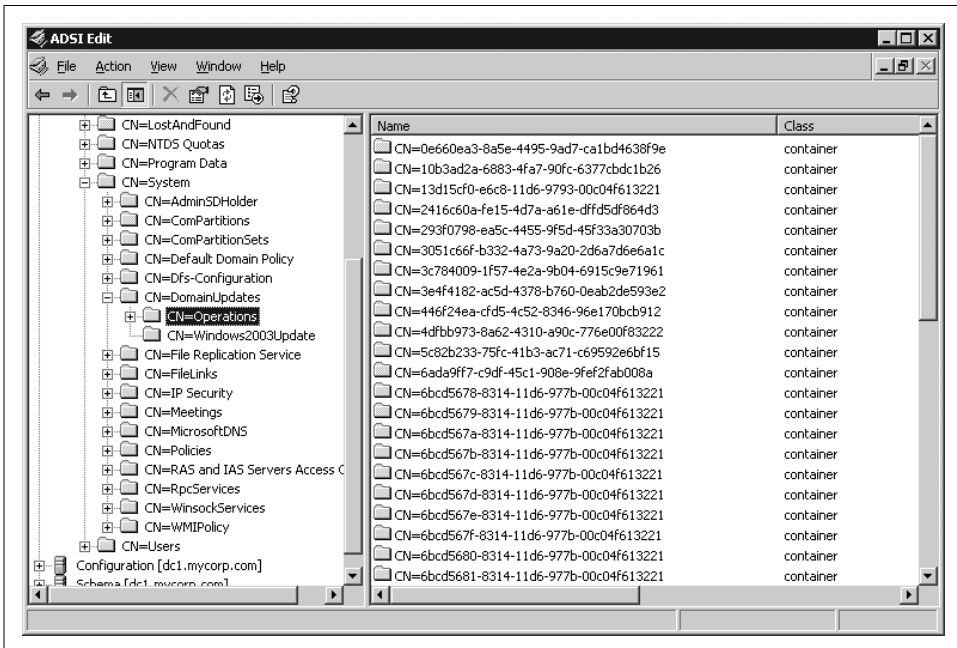


Figure 14-4. ADPrep domain update operations

Once you've run both ForestPrep and DomainPrep and allowed time for the changes to replicate to all domain controllers, you can then start upgrading your domain controllers to Windows Server 2003 or installing new Windows Server 2003 domain controllers.

Upgrade Process

The upgrade process to Windows Server 2003 should be straightforward for most deployments. No forest restructuring is required, no user profile or workstation changes are necessary assuming you are running the latest service pack and hotfixes, and there should be no need for political turf battles over namespace usage and ownership like there might have been with Windows 2000.

We are going to outline five high-level steps that you should follow to upgrade to Windows Server 2003. They include performing an inventory of your domain controllers and clients to determine if there will be any compatibility showstoppers. You are then ready to do a trial run and perform extensive testing to see what impact the upgrade may have on functionality. Next, you have to prepare your forest and domains with ADPrep, which we've already discussed in some depth. Finally, you'll

upgrade your domain controllers to Windows Server 2003. In the “Post Upgrade Tasks” section, we will describe what to do after you’ve upgraded your domain controllers as far as monitoring, raising functional levels, and taking advantage of new features goes.

Inventory Domain Controllers

A good first step before you start the upgrade process is to do a complete inventory of all of the hardware and software that is on your domain controllers. You’ll then want to contact your vendors to determine whether they’ve already done compatibility testing and can verify support for Windows Server 2003. The last thing you want to do is start the upgrade process and find out halfway through that a critical monitoring application or backup software that runs on your domain controllers does not work correctly. Much of this testing can be done in your own labs, but it is always good to check with the vendors and get their seal of approval. After all, if a problem does arise, you’ll want to make sure they are supporting the new platform and won’t push back on you.

Next you’ll want to ensure you have all the necessary hotfixes and service packs installed. A good overview of Microsoft’s recommendations is documented in Microsoft Knowledge Base Article 331161. What you need to install depends on how long you plan on having your Windows 2000 domain controllers around. If you plan on a quick upgrade, you’ll only need to do the minimal amount of patching required. But if you are going to have a prolonged migration, you should consider applying all the current fixes and service packs.

After you are sure that your hardware and software is fully up to date and will work under Windows Server 2003, you’ll then want to do a very thorough check of your current domain controllers and make sure they are running without error. Go through the event logs and resolve any errors and warnings that may be occurring. The *dcdiag* and *netdiag* commands are useful for identifying potential issues. Also, if you don’t already trend CPU and memory statistics, you’ll need to start. The reason for collecting all this data is that if problems occur after the upgrade to Windows Server 2003, you’ll want to narrow it down to whether it was previously a problem or if it is new, most likely as a result of the upgrade. If you don’t collect this data, you are setting yourself up for trouble.

A good compatibility test is to run the `/checkupgradeonly` switch with the Windows Server 2003 installer (*winnt32.exe*).

```
X:\> i386\winnt32.exe /checkupgradeonly
```

This command will go through the steps as if you were upgrading, but it will check only the applications you have installed and the status of the forest. If you have not run ADPrep yet, it will return an error about that.

At this point you'll also want to check the status of your backups. Before you run ADPrep you should have successful backups for at least two domain controllers in every forest and every FSMO role owner. You should also ensure that your disaster-recovery procedures are well documented and have been tested.

Inventory Clients

The good news as far as clients go is that there aren't a lot of requirements for them to work in a Windows Server 2003 forest. In fact, there are no changes required for Windows XP and Windows 2000 machines. For NT 4.0 clients, you should have at least Service Pack 3, and Microsoft recommends Service Pack 6a. For Windows 98 and Windows 95 clients, they will need the DS Client installed as described in Microsoft Knowledge Base Article 323466 or to have their OS upgraded to Windows 2000 or later (not a bad idea anyway if you can get away with it).

Other than that, your clients are fine as is. That said, any wise AD administrator would make sure the clients are thoroughly tested before starting the upgrade. Especially with a new version of Active Directory, there are undoubtedly issues that have yet to be discovered, and you don't want to be the first to find them after you've already upgraded!

Trial Run

While we can go on all day about how easy the upgrade process is, the proof is in the proverbial pudding. We consider it a mandatory step that before you upgrade your first production domain controller to Windows Server 2003, you go through extensive testing in a "production-like" Active Directory forest. So what do we mean by "production-like"? That depends on how much time and resources you have. Perhaps the best way to simulate your production environment is to actually take a production domain controller from each domain in the forest off of the network and put it on a private network. You can then build up the forest on the private network, and all the data that is in production is now in the test environment you just set up. Before we go any further, we want to make it clear that this is the most painstaking option for building a test network, because Active Directory does not self-heal after you put the domain controller on the private network. In fact, you may encounter problems getting the DC to work at all since it cannot initially contact any of the FSMO masters. Microsoft has stated that they'd like to make this process easier and even suggested they may document how to do it, but at the time of publication of this book, nothing of the sort was available. Your other alternative is to populate the test forest with as much of the data from production as possible. If you already have provisioning scripts or a metadirectory that feeds your production Active Directory environment, you may be able to utilize a similar process to populate the test forest.

Once you have a test forest that simulates production up and running, you should add as many clients as possible that represent your users and the various operating systems you support. If you are running Exchange 2000, you should also install it, along with any other directory-enabled applications. Sounds tedious? It is necessary to cover your bases no matter how trivial Microsoft says the upgrade will be. The last thing you want to happen is a major blow-up and then having to explain to your CIO that you didn't do very extensive testing because Microsoft said the upgrade was easy.

The key with the trial run is to document everything thoroughly. If you see anomalies, be sure to document them and follow up to determine whether it is going to be a problem. By the time you are done with the trial-run period, you should have an end-to-end document that describes how you are going to upgrade, how long you plan to wait before you raise functional levels, and in what priority you are going to enable new features.

Prepare the Forest and Domains

As we outlined earlier, before you can promote the first Windows Server 2003 domain controller into your forest, you have to run the ADPrep command. After you've done the DC and client inventories and determined there are no showstoppers to moving forward, you should run ADPrep.

First, you must run ADPrep /forestprep, and after the changes have replicated throughout the forest, you need to run ADPrep /domainprep in every domain. Pretty easy, right? There are a couple of gotchas to be aware of with the schema.

Exchange 2000

If you've installed Exchange 2000 into the forest before running ADPrep, you have to correct some mistakes that were made in the Exchange 2000 schema extensions. Specifically, both ADPrep and Exchange 2000 define labeledURI, houseIdentifier and secretary attributes, but Exchange 2000 does not use the correct LDAP display names (LDAPDisplayName) as defined in RFC 2798. If you run ADPrep after Exchange 2000 has been installed without fixing these attributes, you can end up with duplicate schema objects with different LDAPDisplayName attributes. To solve the problem, you must run the *inetorgpersonfix.ldf* file that is located in `\support\tools\support.cab`. This LDIF file fixes the LDAPDisplayName attributes of the three attributes.

First save the *inetorgpersonfix.ldf* file, then import it using the *ldifde* utility. Here is an example where we will be importing into the *mycorp.com* forest:

```
ldifde.exe /i /f inetOrgPersonFix.ldf /c "DC=X" "DC=mycorp,DC=com"
```

Note that *inetorgpersonfix.ldf* uses DC=X as the forest path, which is why we needed to use the /c switch to replace it with our own forest path.

SFU 2.0

If you've installed Microsoft Services For UNIX (SFU) 2.0 in your Windows 2000 forest, you can run across a similar to issue as the one just described with Exchange 2000. The problem again comes back to an incorrectly defined attribute. In this case it is the uid attribute. Microsoft has developed a hotfix for this issue, which is described in Microsoft Knowledge Base Article 293783.



This applies only to SFU 2.0. If you are running SFU 3.0, you will not encounter this problem.

Upgrade Domain Controllers

Now comes the easy part. You may be wondering how we could possibly say that doing the upgrade is the easy part. Perhaps we should preface it with this: if you've done all your homework, this will be the easy part. All of the hard work comes from doing the DC and client inventory, checking for compatibility issues, monitoring, checking event logs, getting a representative baseline, performing mock upgrades, etc. By the time you get the point of actually doing the upgrades in production, it should be second nature to you.

You can proceed with the upgrade process as slowly or as quickly as you want. Windows Server 2003 domain controllers are fully compatible with Windows 2000 domain controllers. They can also serve any role in a forest, including acting as a global catalog server, any FSMO master, ISTG or Bridgehead server.

Post-Upgrade Tasks

After you've upgraded one or more of your domain controllers to Windows Server 2003, you need to do some additional tasks to fully complete the migration. First and foremost, you need to monitor the domain controllers every step of the way and especially after they have been upgraded. You are setting yourself up for failure if you are not adequately monitoring Active Directory.

Monitor

The criticality of monitoring cannot be overstated. If you are not monitoring, how can you determine whether something broke during the upgrade? Here are several things you should check after you upgrade your first domain controller in a domain, any FSMO role owner, and after all DCs have been upgraded:

Responds to all services

Query LDAP, Kerberos, GC (if applicable), and DNS (if applicable) and be sure authentication and login requests are being processed. The *dcdiag* command can run many of these tests.

Processor and Memory utilization

Trend processor and memory utilization for some period before you do the upgrade so you can compare to the numbers after the upgrade.

DIT growth

The growth of the DIT should not be significant. You may in fact want to do an offline defrag after the upgrade to reclaim any space due to single-instance store of ACLs.

Event logs

This is a no-brainer, but you should always check the event logs to see whether any errors are being logged.

DC resource records registered

Ensure that all of the SRV, CNAME, and A records for the domain controllers are registered. The *dcdiag* command can perform these checks.

Replication is working

Run `repadmin /showreps` and `repadmin /replsum` and watch for anything out of the ordinary.

Group Policies are being applied

You may want to add a new setting to an existing GPO or create a new GPO and see if the settings apply on a client that should be receiving it.

NETLOGON and SYSVOL shares exist

This can consist of opening an Explorer window and browsing the available shares on the domain controller.

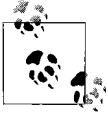
FRS is replicating correctly

You can test this out by placing a test file in the SYSVOL share on a domain controller and waiting for it to replicate to the other domain controllers.

This is not a comprehensive list of everything you should possibly monitor, but it is a good start. If everything checks out over a period of a week, you can feel pretty comfortable that the upgrade was successful. If nothing else, as long as you keep a close eye on the event logs, you should be able to catch the majority of problems.

Raise Functional Levels

After you feel comfortable that the upgrades have completed successfully, your next step should be to start raising the functional levels. If you've only upgraded the domain controllers in a single domain, you can raise the functional level for only that domain to Windows Server 2003. If you've upgraded all the domain controllers in the forest, you can also proceed to upgrade the forest functional level to Windows Server 2003.



If you want to err on the side of caution, and you support multiple domains, you may want to raise the functional level of a single domain and repeat the monitoring steps over a week before raising the forest functional level.

After you raise the functional level of a domain or forest, you should add some additional steps to what you monitor to include testing out new features in Windows Server 2003. For example, to test the Windows Server 2003 domain functional level, you should log on to a domain controller and view the `lastLogonTimestamp` attribute of your user object that we discussed earlier in the chapter. This is a new replicated attribute that will contain your logon time. If after a period of time, you don't see that attribute getting populated, you'll need to dig deeper to determine what is going on.

Perhaps the easiest test to determine whether a functional level has been set for a domain or forest is to query the Root DSE and look at the `domainFunctionality` and `forestFunctionality` attributes. A value of 2 indicates the domain or forest is at the Windows Server 2003 functional level.

Tweak Settings

Once the functional levels have been defined, you'll want to tweak any settings that you discovered during your testing that are set differently than what you want or what you have configured previously. Of special interest should be the settings related to security and account lockout. If you need to disable SMB Signing, you can do so via Group Policy in the Domain Controller Policy → Windows Settings → Security Settings → Local Policies → Security Options → Digitally Sign Communications.

A common pain point for Windows 2000 Active Directory administrators was account lockouts. All of the bug fixes that were incorporated into Service Packs 2 and 3 are included in Windows Server 2003. You may want to revisit your account lockout and password expiration settings. Microsoft's recommendations are included in their Security Template file located at `%SystemRoot%\security\templates\SECURED.C.INF` on a Windows Server 2003 domain controller.

If you had to hardcode any settings on domain controllers in the Registry, you should reevaluate those settings to see whether you still need them. For example, many people increased the intrasite replication frequency from 5 minutes to 15–60 seconds. With Windows Server 2003, the default frequency has changed to 15 seconds.

Start Implementing New Features

After you've upgraded your domain controllers and raised the functional level of a domain or forest, you are ready to start taking advantage of the new features. Some

of them, such as the MMC and CLI enhancements, you can start utilizing immediately. With others, such as quotas, you'll want to think out exactly how to implement them and have them properly documented and communicated before you start using them. If you are using AD-Integrated DNS zones, you should look at converting to application partitions to store DNS data. This is a fairly easy conversion that can be done with the DNS MMC snap-in. In some cases, you may need to completely rethink your current processes. For example, if you start using the "Install from media" feature, you may change how you build and deploy domain controllers.

Summary

In this chapter, we covered the new features in Windows Server 2003 and some of the differences with Windows 2000, most of which were instigated by real-world deployment issues. We then went over how you can enable new features with the use of functional levels and why they are necessary. Next we discussed the ADPrep process and how that must be done before the first Windows Server 2003 domain controller can be promoted. Once you have your forest and domains prepared, you can start the upgrade process. We described some of the important issues to be aware of when upgrading, and finally what to do after you've completed the upgrade.

While this chapter focused mainly on upgrading from an existing Windows 2000 Active Directory infrastructure, in the next chapter we discuss some of the key issues with migrating from Windows NT straight to Windows Server 2003 Active Directory.

This material has been adapted from *Active Directory, 2nd Edition* by Robbie Allen and Alistair G. Lowe-Norris, published by O'Reilly Media, Inc. Copyright O'Reilly Media, Inc., 2003. All rights reserved. To purchase this or other O'Reilly publications, [click here](#).

Additional resources

- Sign up for the [Windows 2000 Server newsletter](#)
- Sign up for the [Windows Server 2003 newsletter](#)
- See all of [TechRepublic's newsletter offerings](#)
- [Ten great Windows Server hacks](#) (TechRepublic)
- [Active Directory: Lock it down in 10 steps](#) (TechRepublic)
- [Build a virtual Active Directory lab with VMware](#) (TechProGuild)