

# LAMPIRAN

## **LAMPIRAN A**

### **Windows 2003 Migration, in a Nutshell**

## Windows 2003 Migration, in a Nutshell

Reader wants the simplest path to upgrade to Windows Server 2003 and Exchange 2003.

by Bill Boswell -- August 2004



**Question:** We're thinking of moving into a Windows Server 2003 environment. Currently, we're running Windows 2000 along with Exchange 2000.

I have two scenarios for doing the upgrade, and I'm trying to decide which one would be the most beneficial for the company. We're going to work out any bugs in the lab by installing a new Windows Server 2003 domain and new Exchange 2003

servers.

Once we're done testing, my boss wants me to join this lab domain to the production domain and then upgrade the production domain. I'd like to work out the bugs in the lab, as well, but then I'd like to upgrade the production domain rather than merge it with the lab domain. Am I being too careful?

Also, we're thinking of deploying Outlook 2003 at the same time as the Exchange 2003 upgrade. Should we wait until we've finished the deployment or do both jobs at the same time?

— *Wilson*

**Answer:** The sequence of events outlined by your boss has one fatal flaw: You can't "join" one Active Directory domain to another regardless of the Windows Server version you're running. There is no merge and purge capability in Active Directory.

To introduce the lab domain into production, you would have to migrate all user, group and computer accounts to the lab domain and re-permission all servers and do other work involving desktop profiles and so forth. That's too much work for a simple *e-mail* migration.


Here's a sequence of operations that would get you to your goal of upgrading the production domain:

1. Make sure that all your applications (including but not limited to antivirus, antispam, backup agents, monitoring agents) and storage interfaces (SCSI, SAN, NAS, iSCSI) work with Windows Server 2003 and Exchange Server 2003. Windows 2003 includes quite a few security upgrades, so make sure you test any applications that rely on Windows authentication.
2. Apply the Inetorgperson hotfix as described in Knowledge Base article [314649](#), "Windows Server 2003 adprep /forestprep

Command Causes Mangled Attributes in Windows 2000 Forests That Contain Exchange 2000 Servers"

<http://support.microsoft.com/default.aspx?scid=kb;en-us;314649>.

3. Run Windows 2003 forestprep and domainprep.
4. Introduce a new Windows 2003 *domain controller* in production.
5. Migrate the remaining *domain controllers* to Windows 2003. Don't upgrade existing DCs. Demote, reformat and reinstall.
6. Run Exchange 2003 forestprep and domainprep.
7. Install the new Exchange 2003 servers. Once again, don't upgrade the existing Exchange 2000 servers. You get the best mix of performance and security by installing newly configured servers.
8. Move *mailboxes*, connectors and public folders to the Exchange 2003 servers. The improved, multithreaded "Move *Mailbox*" feature in Exchange 2003 will help speed the transition, and there's a public folder migration utility in the suite of tools associated with Exchange 2003 SP1 that helps to migrate public folders.
9. Decommission the Exchange 2000 servers. This is relatively straightforward. Once you're sure that you've moved all the public folders and *mailboxes*, take it off the wire for a few days to make sure you got everything, then put it back on the wire and remove Exchange using Add/Remove Programs. This removes the server from the Organization.

As for the Outlook 2003 deployment, you can do the work any time that's convenient for users. Outlook will determine the new location of the user's *mailbox* following a move, so there's no reason why you can't start the Outlook 2003 upgrade today. You won't get all the cool benefits (MAPI compression, drizzle downloads) until you upgrade to Exchange 2003, but you won't hurt your current Exchange servers by using Outlook 2003. 

*Contributing Editor Bill Boswell, MCSE, is the principal of Bill Boswell Consulting, Inc. He's the author of [Inside Windows Server 2003](#) and [Learning Exchange Server 2003](#) both from Addison Wesley. Bill is also Redmond magazine's "Windows Insider" columnist and a speaker at [MCP Magazine's TechMentor Conferences](#). You can contact Bill about "Windows 2003 Migration, in a Nutshell " at [boswell@101com.com](mailto:boswell@101com.com).*

## **LAMPIRAN B**

### ***Step-by-Step: Migrating Exchange 2000 to Exchange 2003 Using New Hardware***

## Step-by-Step: Migrating Exchange 2000 to Exchange 2003 Using New Hardware

Migrate your *mail* system from Exchange 2000 Server running on a Windows 2000 Server system to a new server running Exchange Server 2003 on Windows Server 2003. This scenario will take you through all Exchange-related issues from adding your first Windows Server 2003 system to unplugging your old Exchange 2000 system when finished.

If you simply want to do an in-place upgrade of Exchange 2000 to Exchange 2003 using the same server, you've got it made – Microsoft has explained the process of upgrading and made it pretty simple. Even if you're still using Exchange v5.5, Microsoft has you covered with a wealth of documentation to peruse. But what if you're an Exchange 2000 organization that wants to bring in a new Exchange 2003 system alongside your existing machine, move all your content over to it, and decommission the original box? Then you're left scratching your head. At the time of this writing, there is no guide I've been able to find that explains the process with any detail.

This document will explain the process, combining information from numerous sources as well as my own experience. It's very easy to bring Exchange Server 2003 into your Exchange 2000 organization, with minimal disruption to your existing server or your users. This document assumes you have an Exchange 2000 organization running in native mode.

Henceforth, the Exchange 2000 system will be referred to as the "old" server, and the Exchange 2003 system will be referred to as the "new" server.

### I. Prepare your Network for Windows Server 2003

Regardless of how you intend to get to Exchange 2003, there are some basic steps that must be done.

1. Begin by reviewing Microsoft's [314649 – "Windows Server 2003 adprep /forestprep Command Causes Mangled Attributes in Windows 2000 Forests That Contain Exchange 2000 Servers"](#) This article explains that if you have Exchange 2000 installed in your organization, and you proceed with installing your first Windows Server 2003 system (and its accompanying schema modifications), you may end up with some mangled attributes in AD. Preventing this from happening is simple enough: a script called `Inetorgpersonfix.ldf` will do the trick.
2. Run **adprep /forestprep** from Windows Server 2003 CD on your Windows 2000 server that holds the Schema master FSMO role. (Of course you'll need to be a member of Schema Admins). Be sure to replicate the changes throughout the forest before proceeding.

3. Run **adprep /domainprep** from Windows Server 2003 CD on your Windows 2000 server. I ran it on the system holding the PDC Emulator FSMO role.
4. Before bringing a new Windows Server 2003 system online, it's a good idea to review your third-party server utilities and upgrade them to the latest versions to ensure compatibility. In my installation, this included the latest versions of BackupExec, Symantec Antivirus Corp. Edition, and Diskeeper.
5. Run **setup /forestprep** from the Exchange Server 2003 CD on the Windows 2000 server that holds the Schema master FSMO role. Replicate the changes throughout the forest.
6. Run **setup /domainprep** from the Exchange Server 2003 CD on a Windows 2000 server. Again, I ran it on the system holding the PDC Emulator role.

## II. Install Windows Server 2003

1. Install Windows Server 2003 on the new server, join it to the domain, then apply all hotfixes to the server to bring it up to date.
2. In AD, move the server object to the desired OU.
3. If you're paranoid like me, you may be tempted to install antivirus (AV) software on your new server at the earliest opportunity. Hold off on that for now.
4. Review Microsoft's [815372 – "How to optimize memory usage in Exchange Server 2003"](#) which explains a number of settings required for Exchange Server 2003. Specifically, you may need to add the **/3GB** and **/userva=3030** switches to boot.ini, or you will have event 9665 in the event log. I also had to change the **HeapDeCommitFreeBlockThreshold** value in the registry at HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ to 0x00040000 as directed in the article.
5. Review Microsoft's 831464 – ["FIX: IIS 6.0 compression corruption causes access violations"](#). I obtained the fix from Microsoft, and you should do the same, as it fixes some nasties that may interfere with OWA.

## III. Install Exchange Server 2003

1. If you have installed any AV software on the new server, stop all AV-related services now, or you may experience a failed Exchange installation as I did.
2. Download the latest copy of the [Exchange Server 2003 Deployment Tools](#), version 06.05.7226 as of this writing.

3. To begin the Exchange Server 2003 install on your new server, run **Exdeploy.hta** after extracting the tools.
4. Choose “Deploy the First Exchange 2003 Server”
5. You’ll want to choose the item for your current environment, which in the context of this article is “You are running Exchange 2000 in native mode and you want to upgrade a server or install the first new Exchange 2003 server.” Choose “Upgrade from Exchange 2000 Native Mode”.
6. Run through the entire checklist and perform all the steps and tests. When you get to Step 9 in Exdeploy, you’ll need to specify the path to the Exchange Server 2003 CD since you’re running Exdeploy from a location other than the CD.
7. Install all the Exchange components unless you have a compelling need to do otherwise.
8. When the install is completed, install Exchange Server 2003 Service Pack 1.
9. When SP1 is completed, run the Exchange System Manager from the Windows Server 2003 system, and you will see your new server listed in the Exchange organization, as well as your old server.
10. The POP3 and IMAP4 services aren’t set to start automatically, so configure them for Automatic startup if desired.
11. If you want to install or enable antivirus software, it’s now safe to do so.

#### **IV. Get Familiar with Exchange Server 2003**

At this point, you now have an Exchange 2003 system running in your existing Exchange organization. Microsoft has done a good job of allowing the two versions to coexist.

Before proceeding with your migration, there are a number of important tasks to consider at this stage. For openers, communicate with your users about the migration if you haven’t already, brief them on the new OWA interface, and by all means *ask them to go through their mailboxes and delete old, unneeded items*. You’ll appreciate this later!

This is a good opportunity to spend some time reviewing your new Exchange server. Even if you spent time learning the new product in a lab environment (as you should have), exploring the system now before proceeding makes sense. Check out the new ESM, move a test *mailbox* to the new server, and try OWA. Go through your old server and take note of any settings you want to configure on the new system such as size limits on SMTP connectors or incoming/outgoing messages, etc. You’ll find that Exchange Server 2003 is configured to block *mail* relaying by default.



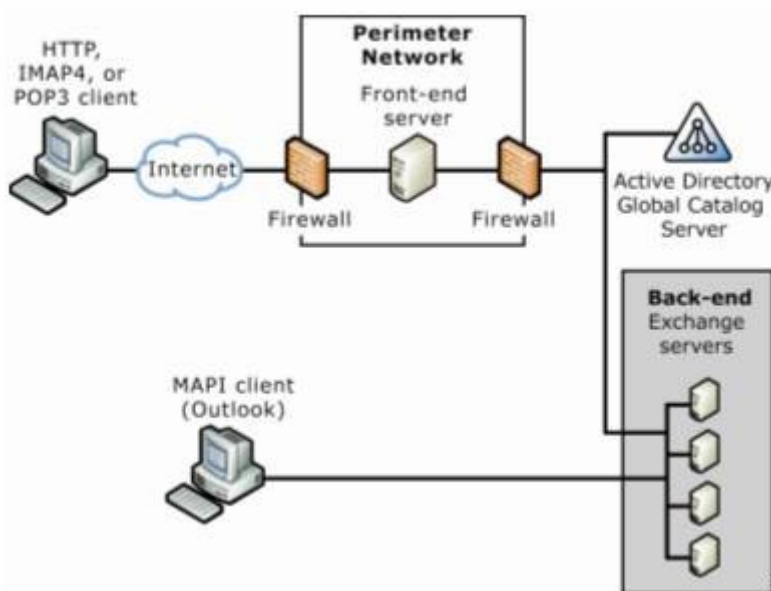
This is a good time to uninstall the Exchange 2000 version of the ESM remote management tools (using the Exchange 2000 Server CD, run Setup, choose Remove) on any management workstations and install the new Exchange 2003 ESM, which can be used to manage both versions of Exchange server.

As you test message routing, you will find that any *email* coming into your organization from the outside will be automatically routed to the appropriate Exchange server where the *mailbox* resides. My test *mailbox* on the new server could send and receive *mail*, no problem. I could also access the *mailbox* with Outlook or OWA from within the organization, no problem. However, *I was unable to access mailboxes on the new server from outside the organization.*

In my configuration, an ISA Server 2000 system acts as the firewall, where web and server publishing rules exist to redirect incoming traffic to the old *mail* server. There was no simple way I could find to allow simultaneous access to both the old and the new servers. All incoming *mail*-related traffic was directed to the old server. This limitation affected the rest of the migration as you will see.

**Note:**

There is a way to have multiple Exchange servers, both 2000 and 2003, behind a firewall, whereby *mail* is automatically directed to the appropriate server. This scenario involves installing Exchange Server 2003 on a server and configuring it as a “front end” server, which allows it to act as a proxy. Unfortunately, the front end server cannot hold any *mailboxes* on its own, so this isn’t an option in the migration scenario in this article.



**Note:**

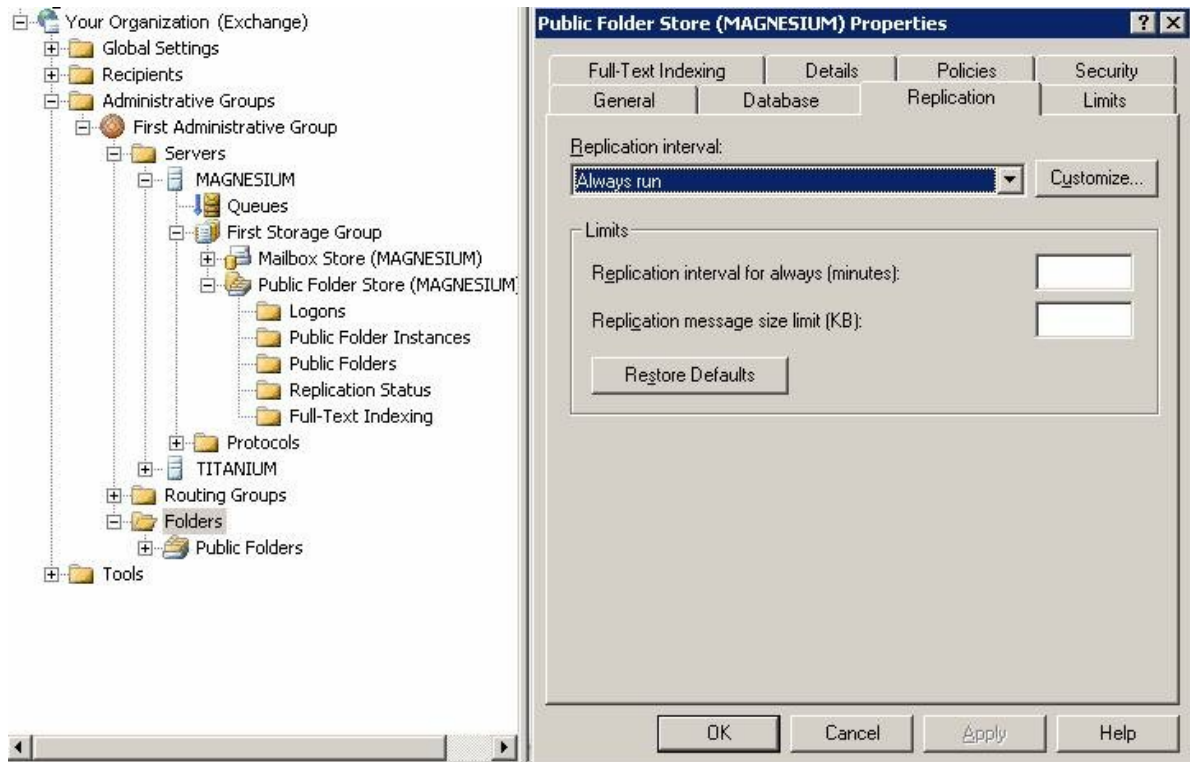
For a front end server to make any sense, a minimum of three servers would be needed: the front end server itself, and at least two Exchange servers, to which the front end server would route messages, based on the *mailboxes* homed on each. In our migration scenario, one could have a front end server routing *mail* to

the old Exchange 2000 server and the new Exchange 2003 server. As *mailboxes* are moved from the old to the new server, the front end server would route messages to the correct place. This is a nice option for those with the hardware and the desire to do a gradual transition.

## V. Configure Exchange Server 2003 to Host Public folders and Other Roles

As you begin moving folders and roles to the new server, one thing I learned the hard way is that you should *use the ESM running on the new server*. I used the ESM on a Windows XP remote management workstation, and found that things reported on the workstations's ESM weren't always the same as the Exchange server's ESM.

1. Review Microsoft's [307917 – "XADM: How to Remove the First Exchange 2000 Server Computer from the Site"](#). This document contains most of what is needed to finish this migration, and explains in detail how to setup replication of Public folders.
2. Using the instructions in 307917 as a guide, setup replication for all public folders that were created by your organization on your old server. *Do not setup replication for any folders you didn't create, as several of these will not be brought over to the new server*. When the folders you replicated are in sync, remove the old server from the replication tab. These folders now exist solely on the new server. They are accessible to those within your WAN, but are inaccessible outside your firewall.
3. You should find that the Public folders called **default** and **ExchangeV1** are already replicated to the new server. Using Step 2 and 3 in 307917, setup replication to the new server for the folders **Offline Address Book**, **OAB Version 2**, and **Schedule+ Free Busy Information**. If you have a folder called **Internet Newsgroups**, you should replicate that also. This folder is created by the Exchange system, though your organization may not use it.
4. If you check the Properties, Replication tab on your administrative group's Folders node, you will see the replication interval for the public folders. Unless you specifically changed the interval on any individual public folders, they should follow this schedule. "Always run" means replication will run every 15 minutes. There is no "replicate now" option.



5. Using Step 4 & 5 in 307917, rehome RUS and designate the new server as the routing group master.
6. Step 6 and 7 in 307917 didn't apply in my configuration; proceed with those as needed.
7. Using Microsoft's [265293 – "How to Configure the SMTP Connector in Exchange"](#), add the new server to the SMTP connector, remove the old server, then cycle the MS Exchange Routing Engine service and the SMTP service for these changes to take effect. Send a test message to verify the new server is sending the *mail* now.
8. There are a number of public folders on the Exchange 2000 server that do not need to be replicated and moved to the new server, including several that are part of the Exchange 2000 version of OWA. On my system these included:
  - Controls
  - Event Config\_<old server name>
  - Events Root
  - Exchweb
  - Img
  - Microsoft

- Offline Address Book – First Administrative Group
- Schema-root
- Views

Just leave these folders on the old server.

At this point, with the exception that your public folders are no longer accessible outside your firewall, there shouldn't be any noticeable difference to your users. You can accomplish all of the above during normal working hours without much fuss. However, the next step isn't as transparent.

## VI. Move the *Mailboxes* to Exchange Server 2003

This is the moment we've all been waiting for, and it's pretty straightforward. In order for this process to go as smoothly as possible, you should make sure that no users inside your organization are accessing the *email* system. You should also block all external access to your *mail* servers.

1. You can read a detailed description of moving *mailboxes*, see Henrik Walther's ["Moving Mailboxes with the Exchange 2003 Move Mailbox Wizard"](#) article for specifics.
2. Prevent outside access to your *mail* servers. In my case, this involved disabling the web and server publishing rules for IMAP4, POP3, and SMTP in my ISA Server 2000 system.
3. Make sure no internal users are accessing the *mail* server.
4. Turn off AV on both the old and the new server. Moving *mailboxes* is a time-consuming, resource-intensive process. AV scanning will slow this process down, and in some cases can cause problems when large scale data is being moved.
5. The Move *Mailbox* Wizard will allow you to select many *mailboxes* at a time, but it will only process four at a time. I chose the "Create a failure report" option, which won't move the *mailbox* if there are errors. I moved 75 *mailboxes*, 1.7GB of data, in 70 minutes, without a single error.
6. The key determining factor in the speed of the *mailbox* move process isn't so much size as it is the number of items in a *mailbox*. If your users deleted a lot of items per your request, the process will go a lot quicker now.
7. If you want to test your new system before moving all the *mailboxes*, you can move a handful of them, then turn on outside access (I would turn on AV as well). Keep in mind, you'll need to configure your firewall to point to the new *mail* server. You should be able to access the new *mailboxes* with OWA and POP3 *mail* applications like Outlook. You can also test access to

Public folders in OWA if desired. Be sure to disable external access and AV before proceeding.

8. Move all the *mailboxes*, except **SystemMailbox**, **System Attendant**, and **SMTP-ServerName**, as these should already exist on the new server.
9. When the process is finished, configure your firewall to point to the new *mail* server, turn on AV, and enable external access. You are now running an Exchange Server 2003 *mail* system.

## VII. Final Cleanup

1. Go through the public folders on the new server and remove the old server from the replication tab for any public folders that are still replicating to it. On my system this included **default** and **ExchangeV1**.
2. Have your clients logon to their *email* clients. Outlook will attempt to connect to the old *mail* server, but as long as the Exchange services are still running on it, it will automatically redirect Outlook to the new server.
3. Stop all the Exchange services on the old server. Stop IISAdmin, which should stop FTP, NNTP, SMTP, and WWW.
4. Your old server will still appear in the Exchange organization in the ESM, but that's OK for now. You may also see an entry in the Queues node on the new server, destined for the old server. You can ignore this also.
5. Allow your new server for run for a few days if desired, keeping the old system in its present state for the time being. You may even want to turn it off.
6. When you're satisfied that the migration is a success and the old server is no longer needed, insert the Exchange 2000 Server CD into the old server, run setup, and remove/uninstall Exchange 2000. Make sure the server is still connected to the network when you do this, as this process will remove the old server from the ESM.

Congratulations! Because you began with an Exchange 2000 organization in native mode, your Exchange Server 2003 system is in native mode. Your migration is finished

## **LAMPIRAN C**

***How to use Active Directory Migration Tool v2.0 to migrate from Windows  
2000 to Windows Server 2003***

## **How to use Active Directory Migration Tool v2.0 to migrate from Windows 2000 to Windows Server 2003?**

This article describes how to set up the Active Directory Migration Tool (ADMT) to migrate from a Windows 2000-based domain to a Windows Server 2003-based domain.

Warning: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

You can use ADMT to migrate users, groups, and computers from one domain to another, and analyze the migration affect before and after the actual migration process.

## **How to Set Up ADMT for a Windows 2000 to Windows Server 2003 Migration**

You can install the Active Directory Migration Tool version 2 (ADMTv2) on any computer that is running Windows 2000 or later, including:

- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional
- Microsoft Windows Server 2003

The computer on which you install ADMTv2 must be a member of either the source or the target domain.

### **Intraforest Migration**

Intraforest migration does not require any special domain configuration. The account you use to run ADMT must have enough permissions to perform the actions that are requested by ADMT. For example, the account must have the right to delete accounts in the source domain, and to create accounts in the target domain.

Intraforest migration is a move operation instead of a copy operation. These migrations are said to be destructive because after the move, the migrated objects no longer exist in the source domain. Because the object is moved instead of copied, some actions that are optional in interforest migrations occur automatically. Specifically, the sidHistory and password are automatically migrated during all intraforest migrations.

### **Interforest Migration**

ADMT requires the following permissions to run properly:

- Administrator rights in the source domain.
- Administrator rights on each computer that you migrate.
- Administrator rights on each computer on which you translate security.

Before you migrate a Windows 2000-based domain to a Windows Server 2003-based domain, you must make some domain and security configurations. Computer migration and security translation do not require any special domain configuration. However, each computer you want to migrate must have the administrative shares, C\$ and ADMIN\$.

The account you use to run ADMT must have enough permissions to complete the required tasks. The account must have permission to create computer accounts in the target domain and organizational unit, and must be a member of the local Administrators group on each computer to be migrated.

### **User and Group Migration**

You must configure the source domain to trust the target domain. Optionally, the target may be configured to trust the source domain. While this may ease configuration, it is not required to finish the ADMT migration.

#### Requirements for Optional Migration Tasks

You can complete the following tasks automatically by running the User Migration Wizard in Test mode and selecting the migrate sIDHistory option. The user account you use to run ADMT must be an Administrator in both the source and the target domains for the automatic configuration to succeed.

1. Create a new local group in the source domain that is named %sourcedomain%\$\$\$. There must be no members in this group.
2. Turn on auditing for the success and failure of Audit account management on both domains in the Default Domain Controllers policy.
3. Configure the source domain to allow RPC access to the SAM by configuring the following registry entry on the PDC Emulator in the source domain with a DWORD value of 1:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\
Control\LSA\TcipClientSupport
```

You must restart the PDC Emulator after you make this change.

Note: For Windows 2000 domains, the account you use to run ADMTv2 must have domain administrator permissions in both the source and target domains. For Windows Server 2003 target domains, the 'Migrate sIDHistory' may be delegated. For more information, see Windows Server 2003 Help & Support.

You can turn on interforest password migration by installing a DLL that runs in the context of LSA. By running in this protected context, passwords are shielded from



being viewed in cleartext, even by the operating system. The installation of the DLL is protected by a secret key that is created by ADMTv2, and must be installed by an administrator.

To install the password migration DLL:

1. Log on as an administrator or equivalent to the computer on which ADMTv2 is installed.
2. At a command prompt, run the `ADMT KEY sourcedomainpath [* | password]` command to create the password export key file (.pes). In this example, `sourcedomain` is the NetBIOS name of the source domain and `path` is the file path where the key will be created. The path must be local, but can point to removable media such as a floppy disk drive, ZIP drive, or writable CD media. If you type the optional password at the end of the command, ADMT protects the .pes file with the password. If you type the asterisk (\*), ADMT prompts for a password, and the system will not echo it as it is typed.
3. Move the .pes file you created in step 2 to the designated Password Export Server in the source domain. This can be any *domain controller*, but make sure it has a fast, reliable link to the computer that is running ADMT.
4. Install the Password Migration DLL on the Password Export Server by running the `Pwmig.exe` tool. `Pwmig.exe` is located in the `I386\ADMT` folder on the Windows Server 2003 installation media, or the folder to which you downloaded ADMTv2 from the Internet.
5. When you are prompted to do so, specify the path to the .pes file that you created in step 2. This must be a local file path.
6. After the installation completes, you must restart the server.
7. If you are ready to migrate passwords, modify the following registry key to have a DWORD value of 1. For maximum security, do not complete this step until you are ready to migrate.

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\

Control\LSA\AllowPasswordExport

The Active Directory Migration Tool v2 is included in the `I386\Admt` folder on the Windows Server 2003 CD.

Download Active Directory Migration Tool v2.0 (4.7mb)

For more information about how to use ADMT to perform a migration, see ADMT Help. Start the Active Directory Migration Tool, click Help Topics on the Help menu, click the Contents tab, and then click Active Directory Migration Tool.

**LAMPIRAN D**

***Top 10 Reasons Why to Upgrade from Windows 2000 Server to Windows  
Server 2003 R2***

# Top 10 Reasons Why to Upgrade from Windows 2000 Server to Windows Server 2003 R2

Windows Server 2003 R2 builds upon the increased security, reliability, and performance provided by Windows Server 2003 Service Pack 1 (SP1) to provide a more secure and dependable platform on which to deliver business-critical applications and Web services. At the same time, Windows Server 2003 R2 is easier to manage and integrate into existing environments. This page describes the major new features and improvements included in Windows Server 2003 R2.

**1 Centralize user authentication and authorization**  
Introduced in Windows 2000, the Active Directory directory service simplifies the administration of complex network directories and makes it easy to locate resources on even the largest networks. This enterprise-class service is scalable, is built on Internet-standard technologies, and integrates with the Standard, Enterprise, and Datacenter editions of Windows Server 2003 R2.

Windows Server 2003 R2 provides numerous ease-of-use improvements to Active Directory and new features, including cross-forest trusts, the ability to rename domains, and the ability to deactivate attributes and classes in the schema so that their definitions can be changed.

**2 Simplify end user policy management**  
Administrators can use Group Policy to define the settings and allowed actions for your users and computers. In contrast with local policy, organizations can use Group Policy to set policies that apply across a given site, domain, or organizational unit in Active Directory. Policy-based management simplifies such tasks as system update operation, application installation, user profiles, and lockdown of desktops.

As an add-in component to Windows Server 2003, the Group Policy Management Console (GPMC) provides the new framework for managing Group Policy. With GPMC, Group Policy becomes much easier to use, a benefit that will enable more organizations to better utilize Active Directory and take advantage of its powerful management features.

**3 Streamline access to external or security-enhanced domains**  
Use Active Directory Federation Services (ADFS) to streamline business-to-business (B2B) communications. ADFS extends the value of Active Directory deployments to facilitate collaboration with partners, resulting in increased user productivity, greater information technology (IT) efficiency, and improved security—and, thus, a greater return on investments made in software.

**4 Schedule point-in-time critical data copies**  
As part of Volume Shadow Copy service, you can configure point-in-time copies of critical data volumes without interrupting service. These copies can then be used for service restoration or archival purposes. Your users can retrieve archived versions of their documents that are invisibly maintained on the server.

5

#### **Deliver more secure and scalable Web application servers**

Enhancements in Windows SharePoint Services, Microsoft .NET Framework 2.0, Windows Server 2003 R2 x64, and Internet Information Services (IIS) 6.0 can help you deliver more secure and scalable Web applications, extend business infrastructure over the Web, and control costs.

Windows SharePoint Services delivers a cost-effective collaboration solution that can be deployed, configured, and managed quickly. It is easily extended to the extranet using ADFS to enable efficient collaboration with partners and customers across organizational boundaries.

ASP.NET enables fast development of rich, DSI-ready (Dynamic Systems Initiative) Web services and applications using the .NET Framework included in Windows Server 2003 R2. Microsoft .NET Framework 2.0 simplifies and accelerates configuration, deployment, and management of more secure, scalable Web applications.

IIS 6.0 delivers a security-enhanced, high-performance Web server that is significantly enhanced by technology offered in Windows Server R2. The highest possible security is ensured by a built-in security advisor. Downtime and errors are greatly reduced with improved debugging capabilities. Finally, x64 supportability allows IIS to deliver more performance for less money.

Internet Information Services (IIS) 6.0 is a full-featured Web server that enables Web applications and XML Web services. IIS 6.0 has been completely re-architected with a new fault-tolerant process model that greatly boosts the reliability of Web sites and applications.

6

#### **Optimize branch office infrastructure**

Windows Server 2003 R2 provides the underlying technologies needed to simplify integration of branch office servers into a larger enterprise IT ecosystem and still provide reliable and consistent access to data for your users. Performance, availability, and productivity—benefits usually associated with a local branch office server—are strengthened, and environmental challenges—such as connectivity limitations and management overhead—are mitigated with the R2 release.

For instance, Windows Server 2003 R2 allows your users to remain productive in the event of a network failure by accessing up-to-date local replicas of remote data and information. The failover with fail-back capabilities in Windows Server 2003 R2 means that if a branch office server fails, branch office users will automatically be connected to a designated failover server, minimizing any disruption. Once the local branch server is up, users will automatically be connected back to their branch server. Bandwidth throttling and scheduling ensures that the most productive use of network bandwidth is made during office hours. Scheduling replication and setting network quotas for replication can minimize the impact of large volumes of data being sent over the wide area network (WAN).

7

#### **Improve storage management**

By using the File Server Resource Manager (FSRM) and Storage Manager for SANs in Windows Server 2003 R2, you can improve storage management across IT resources and optimize storage space on those resources.

## File Server Resource Manager (FSRM)

This feature enables administrators to understand how storage is being used and to manage storage through storage reports, applying quotas to volumes and folders, and screening files on the server. With FSRM, you can better plan and optimize storage by creating quotas, creating file screens, and scheduling storage reports.

## Storage Manager for SANs

This enables customers to provision storage on storage subsystems on a storage area network (SAN). Based on Microsoft Virtual Disk Service (VDS) technology, Storage Manager for SANs allows provisioning on Fiber Channel and Internet SCSI (iSCSI) storage subsystems. This feature is switch and HBA agnostic.

- 8 Enhance application availability**  
The ability to cluster up to (and including) eight nodes is available only in Windows Server 2003 R2 Enterprise Edition and Windows Server 2003 R2 Datacenter Edition. This service provides high availability and scalability for mission-critical applications such as databases, messaging systems, and file and print services.

Clustering works by enabling multiple servers (nodes) to remain in constant communication. If one of the nodes in a cluster becomes unavailable as a result of failure or maintenance, another node immediately begins providing service, a process known as failover. In this event, your users can continue their activities, unaware that service is now being provided from a different server (node).

- 9 Better secure your wireless LAN access**  
Your organization can move to a security model that helps ensure all physical access is authenticated and encrypted, based on the 802.1X support in the Windows Server 2003 family. Support through 802.1X helps ensure that only trusted systems are allowed to connect and exchange packets with security-enhanced networks. Because 802.1X provides dynamic key determination, 802.1X wireless network encryption is dramatically improved by addressing many of the known issues associated with wired equivalent privacy (WEP) used by IEEE 802.11 networks.

This feature provides enhanced security and performance improvements for wireless local area networks (LANs), such as automatic key management, user authentication, and authorization prior to LAN access. It also provides access control for Ethernet networks when wired Ethernet is used in public locations.

- 10 Build the most cost-effective virtual operating environments**  
When you purchase a Windows Server 2003 R2 Enterprise Edition license, you can use the software in one physical operating environment and up to four virtual operating environments simultaneously.

Virtual Server 2005 R2 is ideal for server consolidation and is an ideal way to consolidate multiple workloads onto one physical server. This helps increase efficiency for operations and

hardware usage.

With Windows Server 2003 R2 Enterprise Edition and Virtual Server 2005 R2, customers have a cost-effective server virtualization technology engineered for the Windows Server System platform.

## **LAMPIRAN E**

### ***Microsoft IT Gains Since Implementing Windows Server 2003***

# Microsoft IT Gains Since Implementing Windows Server 2003

Published: June 27, 2004

This article highlights the IT business value gained when Microsoft implemented the Windows Server 2003 operating system. The following stories provide a high-level look at the successes experienced at Microsoft during the rollout and ongoing operations of Windows Server 2003 and are limited to information about the base operating system product.

## IT Business Benefits

By upgrading from Windows Server 2000 to Windows Server 2003, we at Microsoft experienced first-hand the security, reliability, manageability, and performance improvements offered by this operating system.

Based on interviews with IT groups across Microsoft, the following benefits have been recorded since Windows Server 2003 was deployed:

Area	Benefits
Server Consolidation	<ul style="list-style-type: none"><li>• 25-percent server consolidation was achieved by April 2004, and 29-percent consolidation is anticipated by July 2004.</li><li>• 1,500 print queues and 9.5 million pages per month are now served by only four print servers.</li></ul>
Availability	<ul style="list-style-type: none"><li>• Operating system availability study showed 99.9996 percent uptime for Windows Server 2003 over a three-week period.</li><li>• Microsoft Exchange maintained 99.99 percent availability over seven weeks.</li></ul>
Security	Internet Protocol security (IPSec) secure request mode has mitigated risk by segmenting Microsoft IT-managed computers from unmanaged computers at the network level.
Remote Access	<ul style="list-style-type: none"><li>• A 90-percent decrease in Remote Access Service (RAS) server restarts has been noted.</li><li>• 8,300 concurrent RAS connections were made on one day.</li><li>• 16,111 unique remote procedure call (RPC) over Hypertext Transfer Protocol (HTTP) users were recorded in one week in April 2004.</li></ul>
Windows Rights Management Services (RMS)	Since March 2003, 80,000 unique RMS users have been recorded and 1.8 million licenses issued.



Area	Benefits
Active Directory	The database size decreased by more than 5 gigabytes (GB)—35 percent of the original size.

The rest of this article provides more details about the successes experienced across Microsoft as a result of deploying Windows Server 2003.

[↑Top of page](#)

## Windows Server 2003 Technology Stories

What follows are Microsoft IT success stories recorded since Windows Server 2003 was deployed. The following information is based on team interviews with IT groups from across Microsoft.

### Availability and Consolidation

In March 2003, the results of a detailed internal availability test were published. The test compared Windows 2000 with Windows Server 2003 in the Microsoft environment. This three-week test resulted in an operating system availability of 99.9996 percent for Windows Server 2003, compared to 99.986 percent reported for Windows 2000 on a comparable set of servers.

In the past, the Microsoft IT organization built an infrastructure to handle and accommodate instability in the production environment. The greater stability and performance in Windows Server 2003 has allowed for greater streamlining and consolidation. As of April 2004, Microsoft IT consolidated roughly 25 percent of its infrastructure, with a July 2004 goal of a 29-percent consolidation.

### Print

While running Microsoft Windows NT Server 4.0, the Microsoft Redmond campus had 120 servers supporting its printing needs. With Windows 2000, the team was able to reduce that number to 26 servers. And with Windows Server 2003, currently only four servers are in production. More than 1,500 print queues are supported by these four servers, of which two handle 620 public print queues with an average of 9.5 million pages printed per month.

### IPSec

The security of Microsoft's global enterprise network is under continual threat, where untrusted devices present a significant area of risk for both unauthorized access and virus propagation. As of April 29, 2004, network segmentation using IPSec security technology had been deployed to all corporate domains (through secure request mode), requiring that network connectivity to the most trusted assets is verified.

## Domain Controllers

Single Instance Store (SIS), Install From Media (IFM), and *domain controller* rename are just three of the new features in Windows Server 2003 that dramatically improved the ability of Microsoft IT to manage the environment by reducing complexity and increasing operational efficiency:

- **SIS**, an improved method for storing security descriptors, reduced the size of the global catalog database from 14 GB to 9 GB. This decrease reduced the time required for managing disk space through offline defragmentation in addition to allowing for on-disk backups for every *domain controller*.
- Using the on-disk backups, *domain controller* promotions through the **IFM** feature reduced the time required to rebuild a remote server from four days (due to slow links and replication) to less than four hours.
- In Windows 2000, renaming a *domain controller* required demoting and repromoting a server. Over time, naming standards changed, and server replacements resulted in inconsistent naming, which led to operational errors. By using the **domain controller rename** feature, which requires only a single restart, operations teams renamed nearly every *domain controller* in the forest to current standards, reducing errors and bringing consistency to service reporting.

## Active Directory Manageability

Active Directory improvements in Windows Server 2003 provided scalability that enabled password expiration, in one example, to be much more transparent to the Microsoft Identity Management team (IdM), operations teams, Help Desk, and users. Password expiration efficiencies allowed for reduction in staffing requirements to complete the process, compared to Windows 2000, where password expirations required full IdM staff support.

For more information about Active Directory, see the [Active Directory](#) page.

## Windows and Service Pack Deployment

By migrating to Windows Server 2003, Microsoft IT was better able to deploy Windows upgrades and Microsoft IT service packs (IPAKs), which are standardized baseline platforms, using Terminal Services. The number of failed installations due to Terminal Services timeouts decreased by almost 50 percent after Windows Server 2003 was installed across the infrastructure. The ability to establish a connection directly to a server console greatly added functionality and ease both to Windows and IPAK deployments, as well as everyday troubleshooting.

In addition, Windows Server 2003, combined with Remote Management Boards (RMB), enabled Microsoft IT to manage all further deployments and patching from Redmond. This centralization made the change control process much tighter; it

allowed Microsoft IT to react quicker to emergency patching and deployment situations and reduce headcount in the field.

### **Internet Security and Acceleration Server**

The conversion to Windows Server 2003 enabled the Microsoft Internet Security and Acceleration (ISA) Server owners to spend less time managing the patching and operating system level of the servers and more time fine-tuning ISA Server. With Microsoft ISA Server 2004 and Windows Server 2003, Microsoft IT saw a significant improvement in the stability of the servers. This combination has also enabled Microsoft IT to undertake an ambitious project to reduce the number of computers running ISA Server worldwide by 30 percent.

For more information about the features and benefits of ISA Server, see the [ISA Server](#) home page.

### **Remote Access Service**

The improved stability and availability of Windows Server 2003 translates directly into greatly improved service stability for remote access users. This stability has decreased the need for RAS system reboots by 90 percent—and increased availability as detailed in the following example.

In January 2004, severe weather prompted many employees to work remotely, creating an unplanned test of the stability, robustness, and flexibility of the deployed remote access solution, and in particular the virtual private network (VPN) servers. On that day, the solution supported more than 8,300 concurrent remote users with no performance issues. Twenty-five to thirty percent of the total Microsoft Puget Sound community was connected remotely, including critical teams such as the Microsoft IT 24-hour operations teams, software developer groups, finance and human resources organizations, managers, and executives, while the service performed at 98 percent of total designed capacity.

On many VPN servers, the user capacity significantly exceeded 500 ports used—with little impact on performance. In the past when using Windows 2000, demand that neared 400 ports would have very negatively impacted the service.

### **Security**

The default security configuration in Windows Server 2003—specifically, Internet Information Services (IIS)—addresses previous security issues and risks and provides a more secure platform for application integration for applications such as Microsoft Systems Management Server (SMS) 2003. SMS 2003 relies on IIS and its related components and protocols, such as HTTP. With Windows 2000, the development and security teams had to build a security template to improve the security settings of these Windows IIS components, and then ensure that these changes would not negatively impact the transactions of the SMS application. With

Windows Server 2003, these configuration modifications were incorporated as default settings and required no additional configuration after components were installed. As a result, total cost of ownership (TCO) was decreased, but more importantly, the potential for security risks was reduced if post-installation configuration steps were inconsistently executed.

By default, Windows Server 2003 now treats everything except Windows Update as being on the Internet or a high-security zone. There are options to add Trusted and Intranet sites during unattended setup and programmatically using scripts or Group Policy. This provides a safety feature to prevent administrators from inadvertently running unsafe or hostile scripts, executables, applets, and Web controls that might harm or compromise servers.

Another example of an important security upgrade in Windows Server 2003 is the ability to run local services with the least amount of privileges necessary.

### **Exchange Server and Clustering**

With the new capabilities of Windows Server 2003 clustering, the IT messaging team was able to consolidate many servers throughout the Microsoft organization. Along with the new features in Microsoft Exchange and Microsoft Outlook 2003, Windows Server 2003 clustering enabled the team to reduce the number of servers dramatically while increasing availability.

Windows Server 2003 clustering also enabled the team to effectively use enterprise storage solutions and take full advantage of the hardware. Windows clustering enabled worldwide deployments to have between three and seven nodes in a cluster, considerably lowering total cost of ownership and enabling a more centralized approach to administration.

During upgrades, security patches, or other downtime, the IT messaging team can effectively move 4,000 *mailboxes* in a matter of minutes, with little user impact. Before this clustered solution was available, customers experienced from 15 minutes to a few hours of downtime. Windows Server 2003 is also a key factor in obtaining 99.99 percent availability in Exchange for seven weeks.

### **RPC over HTTP**

The RPC over HTTP protocol is a new feature in Windows Server 2003. Outlook 2003 uses it to provide an easy and security-enhanced way for users to remotely access *e-mail*. RPC over HTTP enables users to enjoy the full Outlook experience at home or when traveling with a laptop. All they need is a connection to the Internet and a computer running Microsoft Office 2003, configured for RPC over HTTP. No RAS, smart card, or Outlook Web Access is required.

During the week of April 16, 2004, 16,111 unique users were logged at Microsoft as using RPC over HTTP.

## Windows Rights Management Services

Windows Rights Management Services (RMS) is a Microsoft .NET–connected Web service provided by Windows Server 2003. RMS is a free-of-charge, downloadable software component, available at [Windows Server 2003 Feature Packs](#). RMS works with RMS-enabled applications to provide a means for protecting sensitive information, such as *e-mail* and documents. These rights policies are associated directly with the protected content and remain in place whether the item is forwarded, shared, or even moved to a portable device, such as a CD-ROM, or universal serial bus (USB) drive.

Microsoft IT's RMS infrastructure includes 13 servers in four separate forests. Since March 2003, more than 80,000 unique users have used this technology and more than 1.8 million licenses have been issued.

For more information about this technology, see the [Windows Rights Management Services](#) page.

## Enterprise Storage

Windows Server 2003 includes several new storage features which enable more efficient and cost-effective use of storage assets. The new StorPORT driver was designed for enterprise-class storage platforms and has resulted in improved performance and reliability. The new Multipath I/O (MPIO) framework provides a low-cost, multipath option that allows hosts to access heterogeneous storage arrays. The new Volume Shadow Copy Service feature increases application availability through efficient backup and restore operations and data sharing.

## DNS

Windows Server 2003 introduced to Active Directory application partitions with the built-in ability to migrate DNS records. Leveraging domain-wide DNS application partitions, the replication scope of more than 180,000 objects was limited to the authoritative *domain controllers*. Because DNS objects are the most frequently changed items in the directory, limiting the replication scope increased replication efficiency and reduced network requirements.

Forestwide directory partitions allow all *domain controllers* in the forest to be authoritative for a zone. Because Active Directory replication depends directly on the root domain DNS zone and all global catalog DNS records are held in the root domain zone, by publishing this information to all *domain controllers* in the forest, Microsoft IT removed the requirement that *domain controllers* and users contact a *domain controller* in a root domain. Removing this requirement has increased customer response time and has improved performance during network outages.

## 64-Bit Computing

Microsoft IT has deployed several *domain controllers* on 64-bit platforms, with Itanium-based operating systems currently in production and x64-based operating systems in test. As a result, Microsoft IT reduced the number of *domain controllers* in particular environments while maintaining the level of Active Directory performance to support authentication and directory functionality for applications.

Microsoft IT continues to work with the development teams and other business groups to develop Microsoft SQL Server 2005 64-bit platforms and evaluate 64-bit SAP implementations on the Itanium platform. The x64 architecture greatly interests Microsoft customers as a transitional platform from 32-bit to 64-bit computing, because it supports both environments natively and is expected to be priced competitively against today's traditional P4 Xeon systems.

For more information about 64-bit computing, see the Windows Server 2003 64-Bit Versions page.

## **Hyperthreading**

Windows Server 2003 improves support for Intel 32-bit processors in a manner that enables the operating system and applications to see a single hyperthreading-enabled processor as two CPUs. Code that is written to take full advantage of symmetric multiprocessing (SMP) can run up to 30 percent faster with the feature enabled. Because this is a commodity change to the latest IA-32 processors, there is no price premium. By using Windows Server 2003 on current hardware and enabling hyperthreading, this performance gain is achieved for no additional cost.

## **Memory Management**

The addition of the /USERVA switch in Windows Server 2003 enables more precise control over the kernel-user split of the 4-GB address space. By using this switch, Microsoft IT can tune the operating system more effectively for applications that require or perform better with more user address space. And they can do so while preserving enough kernel resources for critical operating system operations, such as system I/O, better than was possible with only 3 GB.

The more detailed setting of /USERVA=3030 has been successful with the large Exchange servers at Microsoft. This setting provides added user address space to increase the size of the Jet cache. The increased size of the cache improves the performance of the store process, while leaving more non-paged pool (NPP) memory and system page table entries (PTE) than if just 3 GB were used. This leaves more resources for storage and network I/O, both of which are used heavily on the scaled-up Exchange *mailbox* servers at Microsoft.

## **.NET Framework**

Microsoft IT's IPAK has been rewritten for .NET to use the capabilities mentioned previously. For the future, Microsoft IT is also evaluating generic code that

provides functions that behave differently depending on the context in which they are used. Such code also provides integration with the System Definition Model framework, which allows applications and the environment to interact. Self-describing applications and infrastructures communicate their own requirements, constraints, and relationships.

Microsoft IT will be able to model changes, potentially understand their impact before implementation, and then in just one action make all downstream adjustments automatically.

For more information about the System Definition Model, see the [DSI](#) Web site.

### **System32 Tools**

A standardized and fully-supported set of utilities are now available as part of the default operating system installation. In the past, such utilities were available only through feature pack releases, such as optional toolkits, companion CDs, resource kits, or as Web downloads.

In Windows Server 2003 IPAKs, Microsoft IT no longer manages as many internally created tools. These became an administrative burden during beta program cycles, where teams were required to update many tools for each build. The standardized System32 tool set also helps eliminate the earlier problem of differing tool versions with inconsistent features and executables that could get deleted or changed inadvertently by an administrator.

### **Windows Management Instrumentation Capabilities**

Windows Management Instrumentation (WMI) in Windows Server 2003 is more powerful than previous versions, exposing more of the operating system and its services for information collection and management of system configuration.

Microsoft IT now uses WMI scripting and application programming interfaces (APIs) as the preferred way to gather information and manage systems, rather than using external tools and executables. Tracing within the operating system and applications also provides a better view into what is happening at a lower level and the ability to track functionality through multiple processes or applications. As a result, Microsoft IT can better troubleshoot issues and examine performance.

### **Windows Server 2003 Service Pack 1 Additions**

Scheduled for release in the latter half of 2004, Windows Server 2003 Service Pack 1 (SP1) will contain improvements designed to help improve server security, including the following features:

- Windows Firewall is a host-based firewall that can restrict incoming access on a port basis or a protocol basis. A server can be configured to allow incoming communication only to services that the server is designed to provide, reducing the attack surface of the server.
- Enhanced RPC security allows only authenticated RPC calls, which helps to avoid transmissions of worms and other viruses. Today, these worms primarily propagate by way of unauthenticated RPC calls.
- Security Server Roles (SSR) allows for role-based configuration of a system to enable only the necessary services and functions, further reducing the potential attack surface of the server.



**LAMPIRAN F**  
**Supported *Upgrade* Paths**

## Supported Upgrade Paths

Published: April 24, 2003 | Updated: December 6, 2005

When upgrading operating systems, a clean install is recommended as best practice. However, if customers opt to upgrade from a previously installed operating system, they can consult the following table for supported upgrade paths. Locate your current operating system in the left column and scan its row for supported upgrade path options.

Note that localized products cannot be upgraded across languages. For example, the Japanese version of Windows 2000 Server cannot be upgraded by an English version of Windows Server 2003 or Windows Server 2003 R2. Multilingual User Interface-enabled servers, however, can be upgraded by English versions of Windows Server 2003 or Windows Server 2003 R2.

### Supported Upgrade Paths in Windows Server 2003 and Windows Server 2003 R2

Details on this benchmark:					
	Standard Edition (including R2)	Enterprise Edition (including R2)	Datacenter Edition (including R2)	Web Edition	Windows Small Business Server 2003
Windows NT 3.51					
Windows NT 4.0* Server	•	•			
Windows NT 4.0* Terminal Server Edition	•	•			
Windows NT 4.0* Enterprise Edition		•			
Windows 2000 Server	•	•			•
Windows 2000 Advanced Server		•			
Windows 2000 Datacenter Server			•		
Windows Server 2003 Standard Edition or Windows Server 2003	•	•			•

<b>Details on this benchmark:</b>					
	<b>Standard Edition (including R2)</b>	<b>Enterprise Edition (including R2)</b>	<b>Datacenter Edition (including R2)</b>	<b>Web Edition</b>	<b>Windows Small Business Server 2003</b>
<b>R2 Standard Edition</b>					
<b>Windows Server 2003 Enterprise Edition or Windows Server 2003 R2 Enterprise Edition</b>		•			
<b>Windows Server 2003 Datacenter Edition or Windows Server 2003 R2 Enterprise Edition</b>			•		
<b>Windows Server 2003 Web Edition</b>				•	
<b>Windows Server 2003** Beta3/RC1/RC2</b>	•	•	•	•	
<b>Small Business Server 2000</b>					•
<b>Windows Small Business Server 2003</b>					•

\* Windows NT® 4.0 upgrade is supported by Service Pack 5 (SP5) or later. If earlier version of server pack is installed, the upgrade is not possible.

\*\* Interim releases of Windows Server 2003 will upgrade to the release to manufacturer (RTM) code of same edition. For example, RC1 Standard Edition upgrades to RTM Standard Edition.

## **LAMPIRAN G**

### ***Checklist: Creating a new child domain***

## Checklist: Creating a new child domain

Updated: January 21, 2005

### Checklist: Creating a new child domain

Step	Reference
(Optional) Review concepts about adding new child domains.	<a href="#">Creating a new child domain</a>
(Optional) Review concepts about security and other options available when using the Active Directory Installation Wizard.	<a href="#">Using the Active Directory Installation Wizard</a>
Verify that the server on which you will be installing Active Directory has an NTFS partition.	<a href="#">Reformatting or converting a partition to use NTFS</a>
Verify that you are a member of the Enterprise Admins group or the Domain Admins group of the parent domain.	<a href="#">Default groups</a>
Verify that DNS is properly configured before installing Active Directory.	<a href="#">Checklist: Verifying DNS before installing Active Directory</a>
Create the <i>domain controller</i> .	<a href="#">Create a new child domain</a>

## **LAMPIRAN 8**

***Checklist: Creating an additional domain controller in an existing domain***

## Checklist: Creating an additional *domain controller* in an existing domain

Updated: January 21, 2005

### Checklist: Creating an additional *domain controller* in an existing domain

Step	Reference
(Optional) Review concepts about creating additional <i>domain controllers</i> over the network or by using backup media.	<a href="#">Creating an additional domain controller</a>
(Optional) Review concepts about security and other options available when using the Active Directory Installation Wizard.	<a href="#">Using the Active Directory Installation Wizard</a>
Verify that the server on which you will be installing Active Directory has an NTFS partition.	<a href="#">Reformatting or converting a partition to use NTFS</a>
(Optional) Review the role of a <i>domain controller</i> .	<a href="#">Domain controllers</a>
Verify that you are a member of the Domain Admins group in the domain where you will be adding the <i>domain controller</i> .	<a href="#">Default groups</a>
Verify that DNS is properly configured before installing Active Directory.	<a href="#">Checklist: Verifying DNS before installing Active Directory</a>
Create the <i>domain controller</i> .	<a href="#">Create an additional domain controller</a>

## **LAMPIRAN I**

### ***What's New in Active Directory***



## What's New in Active Directory

Published: July 24, 2002 | Updated: November 16, 2005



The Active Directory directory service provides single-logon capability and a central repository for information for your entire infrastructure, vastly simplifying user and computer management and providing superior access to networked resources. This article provides an overview of benefits, new features, and improvements for Active Directory in Windows Server 2003.

### Benefits

Improvements in Active Directory deliver key strategic benefits for medium and large enterprises, enabling greater administrator and user productivity. Expanding on the foundation established in Windows 2000, Windows Server 2003 improves the versatility, manageability, and dependability of Active Directory. Organizations can benefit from further reductions in cost while increasing the efficiency in which they share and manage the various elements of the enterprise.

Benefit	Description
Greater Flexibility	Active Directory introduces important new features ensuring that it is one of the most flexible directory structures in the marketplace today. As directory-enabled applications become more prevalent, organizations can utilize the capabilities of Active Directory to manage the most complicated enterprise network environments. Internet data centers, extranet application deployments, large distributed branch office enterprises – the improvements provided by Windows Server 2003 simplify administration and increase performance and efficiency, making it a very versatile solution.
Reduced Total Cost of Ownership	Active Directory has been enhanced to reduce total cost of ownership (TCO) and operation within the enterprise. New features and enhancements have been provided at all levels of the product to extend versatility, simplify management, and increase dependability.

[↑Top of page](#)

### New Features in Windows Server 2003 R2

With Windows Server 2003 R2, Active Directory enables additional flexible deployment options, facilitating interoperability with Unix environments, extranet application deployments, cross-domain identity federation, and decentralized application directory deployments

Benefit	Description
Active Directory Federation Services (ADFS)	ADFS provides Web-based extranet authentication/authorization, single sign-on (SSO), and federated identity services for Windows Server environments, increasing the value of existing Active Directory deployments in scenarios involving B2C extranets, intracompany (multiforest) federation, and B2B internet federation.
Active Directory Application Mode (ADAM)	Previously available as a Web download, Active Directory Application Mode (ADAM) is now included on the Windows Server media. An independent mode of Active Directory without infrastructure features, ADAM provides directory services for applications. Operating as a stand-alone data store or interacting with an Active Directory <i>domain controller</i> , the flexibility of ADAM enables administrators to tailor their directory services infrastructure to varying degrees of local control/autonomy or shared services.
UNIX Identity Management	UNIX integration helps to establish uninterrupted user access and efficient management of network resources across operating systems, by enabling AD <i>domain controllers</i> to act as master NIS servers, and synchronizing user passwords in Unix and Windows environments.

[↑Top of page](#)

## New Features and Improvements

Windows Server 2003 brings many improvements to Active Directory, making it even more versatile, dependable, and economical to use. Specifically, Active Directory in Windows Server 2003 provides:

- Easier deployment and management.
- Greater security.
- Improved performance and dependability.

## Easier Deployment and Management

Windows Server 2003 enhances the administrator's ability to efficiently configure and manage Active Directory even in very large enterprises with multiple forests, domains, and sites. Improved migration and management tools, along with the ability to rename Active Directory domains, make deploying Active Directory significantly easier than when the directory service was first introduced in Windows 2000 Server. Better tools bring drag-and-drop capabilities, multi-object selection, and the ability to save and reuse queries. Plus, improvements in Group Policy make it easier and more efficient to manage groups of users and computers in an Active Directory environment.

Benefit	Description
ADMT version 2.0	It is now easier to migrate to Active Directory through a number of improvements that have been made to the Active Directory Migration Tool (ADMT). ADMT 2.0 now allows migrating passwords from Microsoft Windows NT® 4.0 to Windows 2000 and Windows Server 2003 or from Windows 2000 to Windows Server 2003 domains.
Domain Rename	This supports changing the Domain Name System (DNS) and/or NetBIOS names of existing domains in a forest, keeping the resulting forest still "well formed." Administrators have greater flexibility in changing the Active Directory structure after it is deployed. Design decisions are now reversible, which benefits organizations that may be involved in a merger or significant restructuring.
Schema Redefine	The flexibility of Active Directory has been enhanced to allow the deactivation of attributes and class definitions in the Active Directory schema. Attributes and classes can be redefined if an error was made in the original definition.
Group Policy Improvements	In conjunction with Windows Server 2003, Microsoft is releasing a new Group Policy management solution that unifies management of Group Policy. The Microsoft Group Policy Management Console (GPMC) provides a single solution for managing all Group Policy-related tasks. GPMC lets administrators manage Group Policy for multiple domains and sites within a given forest, all in a simplified user interface (UI) with drag-and-drop support. Highlights include new functionality such as backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These operations are fully scriptable, which lets administrators customize and automate management. Together these advantages make Group Policy much easier to use and help you manage your enterprise more cost-effectively.
Enhanced UI	As the principal means to manage enterprise identities, objects, and relationships, improved interfaces increase administration efficiency and integration capabilities. Microsoft Management Console (MMC) plug-ins now include drag-and-drop capabilities, multi-object selection, and the ability to save and reuse queries. Administrators may now edit multiple user objects simultaneously, reset access control list (ACL) permissions to the default, show effective permissions on a security principal, and indicate the parent of an inherited permission.

## Greater Security

Additional security features make it easier to manage the multiple forests and cross-domain trusts. Cross forest trust provides a new type of Windows trust for managing the security relationship between two forests—greatly simplifying cross-forest security administration and authentication. Users can securely access resources in other forests without sacrificing the single sign-on and administrative benefits of having only one user ID and password maintained in the user's home forest. This provides the flexibility to account for the need for some divisions or areas to have their own forest, yet maintain benefits of Active Directory. In

addition, a new credential manager provides a secure store of user credentials and X.509 certificates. Software restriction policies let administrators prevent unwanted programs from being installed on computers throughout the network.

<b>Benefit</b>	<b>Description</b>
Cross-Forest Authentication	Cross-forest authentication enables secure access to resources when the user account is in one forest and the computer account is in another forest. This feature allows users to securely access resources in other forests, using either Kerberos or NTLM, without sacrificing the single sign-on and administrative benefits of having only one user ID and password maintained in the user's home forest.
Cross-Forest Authorization	Cross-forest authorization makes it easy for administrators to select users and groups from trusted forests for inclusion in local groups or ACLs. This feature maintains the integrity of the forest security boundary while allowing trust between forests. It enables the trusting forest to enforce constraints on what security identifiers (SIDs) it will accept when users from trusted forests attempt to access protected resources.
Cross-Certification Enhancements	The Windows Server 2003 client cross-certification feature is enhanced by enabling the capability for department-level and global-level cross certifications. For example, WinLogon will now be able to query for cross certificates and download these into the "enterprise trust/enterprise store." As a chain is built, all cross certificates will be downloaded.
IAS and Cross-Forest Authentication	If Active Directory forests are in cross-forest mode with two-way trusts, then Internet Authentication Service/Remote Authentication Dial-In User Service (IAS/RADIUS) can authenticate the user account in the other forest with this feature. This gives administrators the capability to easily integrate new forests with already existing IAS/RADIUS services in their forest.
Credential Manager	The Credential Manager provides a secure store of user credentials, including passwords and X.509 certificates. This will provide a consistent single-sign on experience for users, including roaming users. For example, when a user accesses a line-of-business application within their company's network, the first attempt to access this application requires authentication and the user is prompted to supply a credential. After the user provides this credential, it will be associated with the requesting application. In future access to this application, the saved credential will be re-used without prompting the user.
Software Restriction Policies	Software restriction policies address the need to regulate unknown or untrusted software. With software restriction policies, you can protect your computing environment from untrusted software by identifying and specifying which software is allowed to run. You can define a default security level of unrestricted or disallowed for a GPO so that software is either allowed or not allowed to run by default. You can make exceptions to this default security level by creating rules for specific software.

## Improved Performance and Dependability

Windows Server 2003 more efficiently manages the replication and synchronization of Active Directory information. Administrators can better control the types of information that are replicated and synchronized between *domain controllers* both within a domain as well as across domains. In addition, Active Directory provides more features to intelligently select only changed information for replication—no longer requiring updating entire portions of the directory.

Benefit	Description
Easier Logon for Remote Offices	Branch offices with <i>domain controllers</i> can provide user logon through cached credentials without first contacting the global catalog, improving system performance and robustness over unreliable wide area networks (WANs). The loss of connectivity between a branch office and a global catalog no longer impacts the ability of branch users to log on. Branch offices can be supported more effectively and bandwidth consumption over WAN links is reduced.
Group Membership Replication Enhancements	Some directory information does not need to be made globally available. This feature provides the capability to host data in Active Directory without significantly impacting network performance by providing control over the scope of replication and placement of replicas.
Application Directory Partitions	Some directory information does not need to be made globally available. This feature provides the capability to host data in Active Directory without significantly impacting network performance by providing control over the scope of replication and placement of replicas.
Install Replica from Media	Instead of replicating a complete copy of the Active Directory database over the network, this feature allows an administrator to source initial replication from files created when backing up an existing <i>domain controller</i> or global catalog server.
Dependability Improvements	Active Directory includes several new features that increase dependability such as Health Monitoring, which allows administrators to verify replications between <i>domain controllers</i> , improved global catalog replication, and an updated Inter-Site Topology Generator (ISTG) that scales better by supporting forests with a greater number of sites than Windows 2000.

## **LAMPIRAN J**

### ***Domain controllers***

## **Domain controllers**

Updated: January 21, 2005

### **Domain controllers**

When you create the first *domain controller* in your organization, you are also creating the first domain, the first forest, the first site, and installing Active Directory. *Domain controllers* running Windows Server 2003 store directory data and manage user and domain interactions, including user logon processes, authentication, and directory searches. *Domain controllers* are created by using the Active Directory Installation Wizard. For more information, see [Using the Active Directory Installation Wizard](#) .

### **Note**

- You cannot install Active Directory on a computer running Windows Server 2003, Web Edition, but you can join the computer to an Active Directory domain as a member server. For more information about Windows Server 2003, Web Edition, see [Overview of Windows Server 2003, Web Edition](#) .

When using *domain controllers* in your organization, you will want to think about how many *domain controllers* you'll need, the physical security of those *domain controllers*, a plan for backing up the domain data, and upgrading *domain controllers*.

### **Determining the number of *domain controllers* you need**

A small organization using a single local area network (LAN) might need only one domain with two *domain controllers* for high availability and fault tolerance. A larger organization with many network locations will need one or more *domain controllers* in each site to provide high availability and fault tolerance.

If your network is divided into sites, it is often good practice to put at least one *domain controller* in each site to enhance network performance. When users log on to the network, a *domain controller* must be contacted as part of the logon process. If clients must connect to a *domain controller* located in a different site, the logon process can take a long time. For more information, see [Replication between sites](#) .

By creating a *domain controller* in each site, user logons are processed more efficiently within the site. For information about how to create additional *domain controllers*, see [Create an additional domain controller](#) .

To optimize network traffic, you can also configure *domain controllers* to receive directory replication updates only during off-peak hours. For information about how to schedule site replication, see [Configure site link replication availability](#) .

The best network performance is available when the *domain controller* at a site is also a global catalog. This way, the server can fulfill queries about objects in the entire forest. However, enabling many *domain controllers* as global catalogs can increase the replication traffic on your network. For more information about the global catalog, see [The role of the global catalog](#) . For more information about adding global catalogs to sites, see [Global catalogs and sites](#) .

In domains with more than one *domain controller*, do not enable the *domain controller* holding the infrastructure master role as a global catalog. For more information, see [Operations master roles](#) .

### **Physical security**

Physical access to a *domain controller* can provide a malicious user unauthorized access to encrypted passwords. For this reason, it is recommended that all *domain controllers* in your organization be locked in a secured room with limited public access. You can use additional security measures such as Syskey for extra protection on *domain controllers*. For more information about Syskey, see [The system key utility](#) .

### **Backing up domain controllers**

You can back up domain directory partition data and data from other directory partitions by using Backup, which is included with the Windows Server 2003 family, from any *domain controller* in a domain. By using the backup tool on a *domain controller*, you can:

- Back up Active Directory while the *domain controller* is online.
- Back up Active Directory using batch file commands.
- Back up Active Directory to removable media, an available network drive, or a file.
- Back up other system and data files.

When you use the backup tool on a *domain controller* it will automatically back up all of the system components and all of the distributed services upon which Active Directory is dependent. This



dependent data, which includes Active Directory, is known collectively as the System State data.

On a *domain controller* running Windows Server 2003, the System State data consists of the system startup files; the system registry; the class registration database of COM+ (an extension to the Component Object Model); the SYSVOL directory; Certificate Services database (if installed); Domain Name System (if installed); Cluster service (if installed); and Active Directory. It is recommended that you regularly back up System State data.

For general information about the System State, see [System State data](#) . For more information about how to back up the System State, see [Back up System State data](#) . For more information about how to restore a System State backup, see [Restore System State data](#) .

You can install Active Directory on a server running Windows Server 2003 by using a restored backup taken from a *domain controller* running Windows Server 2003. For more information, see [Creating an additional domain controller](#) .

### **Upgrading *domain controllers***

On *domain controllers* running Windows NT 4.0, you will first need to upgrade the primary *domain controller* (PDC) to successfully upgrade the domain. Once the PDC has been upgraded, you can upgrade the backup *domain controllers* (BDCs). For more information, see [Upgrading from a Windows NT domain](#) .

If you currently have a Windows 2000 forest that does not have any *domain controllers* running Windows Server 2003, you will need to prepare the forest and the target domain before you can upgrade *domain controllers* running Windows 2000. For more information, see [Upgrading from a Windows 2000 domain](#) .

## **LAMPIRAN K**

### **Raise the domain functional level**

## Raise the domain functional level

Updated: January 21, 2005

### To raise the domain functional level

1. Open Active Directory Domains and Trusts.
2. In the console tree, right-click the domain for which you want to raise functionality, and then click **Raise Domain Functional Level**.
3. In **Select an available domain functional level**, do one of the following:
  - To raise the domain functional level to Windows 2000 native, click **Windows 2000 native**, and then click **Raise**.
  - To raise domain functional level to Windows Server 2003, click Windows Server 2003, and then click **Raise**.

### Caution

- If you have or will have any *domain controllers* running Windows NT 4.0 and earlier, then do not raise the domain functional level to Windows 2000 native. Once the domain functional level is set to Windows 2000 native, it cannot be changed back to Windows 2000 mixed.
- If you have or will have any *domain controllers* running Windows NT 4.0 and earlier or Windows 2000, then do not raise the domain functional level to Windows Server 2003. Once the domain functional level is set to Windows Server 2003, it cannot be changed back to Windows 2000 mixed or Windows 2000 native.

### Notes

- To perform this procedure, you must be a member of the Domain Admins group in the domain for which you want to raise functionality or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority. As a security best practice, consider using Run as to perform this procedure. For more information, see [Default local groups](#) , [Default groups](#) , and [Using Run as](#) .
- To open Active Directory Domains and Trusts, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Domains and Trusts**.
- You can also raise the domain functional level by right-clicking a domain displayed in Active Directory Users and Computers, and then clicking **Raise Domain Functional Level**.

- The current domain functional level is displayed under **Current domain functional level** in the **Raise Domain Functional Level** dialog box.

## **LAMPIRAN L**

**Raise the forest functional level**

# Raise the forest functional level

Updated: January 21, 2005

## To raise the forest functional level

1. Open Active Directory Domains and Trusts.
2. In the console tree, right-click the **Active Directory Domains and Trusts** node, and then click **Raise Forest Functional Level**.
3. In **Select an available forest functional level**, click Windows Server 2003, and then click **Raise**.

## Caution

- If you have or will have any *domain controllers* running Windows NT 4.0 and earlier or Windows 2000, then do not raise the forest functional level to Windows Server 2003. Once the forest functional level has been set to Windows Server 2003, it cannot be changed back to Windows 2000.

## Notes

- To perform this procedure, you must be a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority. As a security best practice, consider using Run as to perform this procedure. For more information, see [Default local groups](#) , [Default groups](#) , and [Using Run as](#) .
- To open Active Directory Domains and Trusts, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Domains and Trusts**.
- Windows 2000 native is the minimum domain functionality requirement for raising the forest functional level to Windows Server 2003.
- To raise the forest functional level, you must first upgrade (or demote) all existing Windows 2000 *domain controllers* within your forest.
- If you are unable to 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 need to be upgraded from Windows NT or Windows 2000.
- The current forest functional level is displayed under **Current forest functional level** in the **Raise Forest Functional Level** dialog box.

**LAMPIRAN M**  
**Forest Design Models**

## **Forest Design Models**

Updated: March 28, 2003

You can apply one of the following three forest design models in your Active Directory environment:

- Organizational forest model
- Resource forest model
- Restricted access forest model

It is likely that you will need to use a combination of these models in order to meet the needs of all the different groups in your organization.

### **Organizational Forest Model**

In the organizational forest model, user accounts and resources are contained in the forest and managed independently. The organizational forest can be used to provide service autonomy, service isolation, or data isolation, if the forest is configured to prevent access to anyone outside the forest.

If users in an organizational forest need to access resources in other forests, or vice versa, trust can be established between one organizational forest and the other forests. This makes it possible for administrators to grant access to resources in the other forest.

Every Active Directory design includes at least one organizational forest.

### **Resource Forest Model**

In the resource forest model, a separate forest is used to manage resources. Resource forests do not contain user accounts other than those required for service administration and those required to provide alternate access to the resources in that forest if the user accounts in the organizational forest become unavailable. Forest trusts are established so that users from other forests can access the resources contained in the resource forest.

Resource forests provide service isolation that is used to protect areas of the network that need to maintain a state of high availability. For example, if your company includes a manufacturing facility that needs to continue to operate when there are problems on the rest of the network, you can create a separate resource forest for the manufacturing group.



## **Restricted Access Forest Model**

In the restricted access forest model, a separate forest is created to contain user accounts and data that must be isolated from the rest of the organization. Restricted access forests provide data isolation in a situation for project data for which the consequences of compromise are severe.

Users from other forests cannot be granted access to the restricted data because no trust exists. In this model, users have an account in an organizational forest for access to general organizational resources and a separate user account in the restricted access forest for access to the classified data. These users must have two separate workstations, one connected to the organizational forest and the other connected to the restricted access forest. This protects against the possibility that a service administrator from one forest can gain access to a workstation in the restricted forest.

In extreme cases, the restricted access forest might be maintained on a separate physical network. Organizations that work on classified government projects sometimes maintain restricted access forests on separate networks in order to meet security requirements.

**LAMPIRAN N**

**New Active Directory features in Windows Server 2003 with Service Pack 1  
(SP1)**

## New features for Active Directory

Updated: January 21, 2005

### New Active Directory features in Windows Server 2003 with Service Pack 1 (SP1)

The following list summarizes the Active Directory® directory service features that are new since the original release of Windows Server 2003.

- **Directory service backup reminders.** A new event message, event ID 2089, provides the backup status of each directory partition that a *domain controller* stores, including application directory partitions and Active Directory Application Mode (ADAM) partitions. If halfway through the tombstone lifetime a partition has not been backed up, this event is logged in the Directory Service event log and continues daily until the partition is backed up.
- **Added replication security and fewer replication errors.** Replication metadata for *domain controllers* from which Active Directory has been removed is no longer retained by default, although a waiting period can be configured. This change improves replication security and eliminates replication error messages that are caused by failed attempts to replicate with decommissioned *domain controllers*. For more information about preserving replication metadata, see [How the Active Directory Replication Model Works](#) .
- **Install from Media improvement for installing DNS servers.** Install from Media improvements make it easier to create a new *domain controller* that is a DNS server by providing a new option to include application directory partitions in the backup media that is used to install the new *domain controller*. This option eliminates the requirement for replication of the DomainDNSZones and ForestDNSZones application directory partitions before the DNS server is operational.
- **Enhancements for replication and DNS testing.** The Dcdiag.exe command-line tool, which is available in Windows Support Tools, provides new reporting on the overall health of replication with respect to Active Directory security. This test provides a summary of results, along with detailed information for each *domain controller* that is tested and a diagnosis of any security errors. Dcdiag.exe also has new Domain Name System (DNS) tests for connectivity, service availability, forwarders and root hints, delegation, dynamic update, locator record registrations, external name resolution, and enterprise infrastructure. These tests can be performed on one *domain controller* or on all *domain controllers* in a forest. For more information about using Dcdiag.exe, see [Windows Support Tools Help](#) .
- **Support for running *domain controllers* in virtual machines.** On a single physical server that is running Windows Server 2003 and Microsoft Virtual Server 2005, you can install multiple Windows Server 2003 or Windows 2000 Server *domain controllers* in separate virtual machines. This

platform is well suited for test environments. By using virtual machines, you can effectively host multiple domains, multiple *domain controllers* for the same domain, or even multiple forests on one physical server that is running a single operating system. Windows Server 2003 SP1 also provides protection against directory corruption that can result from improper backup and restore of *domain controller* images. For more information about running *domain controllers* in virtual machines, see [Running Domain Controllers in Virtual Server 2005](#) .

- **Operations master health and status reporting.** If an operation that requires a *domain controller* that holds an operations master role (also known as flexible single-master operations (FSMO)) cannot be performed, events are now logged in the Directory Service event log. Events identify role holders that do not exist, exist but are not available, or are available but have not replicated recently with the contacting *domain controller*. For more information about operations masters, see [How Operations Masters Work](#) .
- **Extended storage of deleted objects.** The default period that a copy of a deleted object is retained in Active Directory, called the tombstone lifetime, is extended from 60 days to 180 days. Longer tombstone lifetime decreases the chance that a deleted object remains in the local directory of a disconnected *domain controller* beyond the time when the object is permanently deleted from online *domain controllers*. The tombstone lifetime is not changed automatically when you upgrade to Windows Server 2003 with SP1, but you can change the tombstone lifetime manually after the upgrade. New forests that are installed with Windows Server 2003 with SP1 have a default tombstone lifetime of 180 days. For more information about tombstone lifetime, see [How the Data Store Works](#) .
- **Improved *domain controller* name resolution.** In response to DNS name resolution failures that may be encountered during location of replication partners and global catalog servers, *domain controllers* running Windows Server 2003 with SP1 request other variations of the server name that might be registered, which results in fewer failures due to DNS delays and misconfiguration. For more information about DNS name resolution, see [How DNS Support for Active Directory Works](#) .
- **Improved server metadata removal.** The Ntdsutil.exe command-line tool for managing the Active Directory database has new functionality that makes it easier to remove *domain controller* metadata. Preliminary steps, such as connecting to a server, domain, and site, are no longer required. You simply specify the server to remove. You can also specify the server on which to perform the deletion. Metadata removal is now more comprehensive: in addition to Active Directory replication metadata, the tool now removes File replication service (FRS) metadata and operations master metadata. If an operations master role is assigned to the server that is being removed, the tool attempts to transfer the role to an appropriate *domain controller*. For more information, see [Delete extinct server metadata](#) .
- **Improved security to protect confidential attributes.** To prevent Read

access to confidential attributes, such as a Social Security number, while allowing Read access to other object attributes, you can designate specific attributes as confidential by setting a search flag on the respective attributeSchema object. By default, only domain administrators have Read access to confidential attributes, but this access can be delegated. For more information about access to attributes, see [How Security Descriptors and Access Control Lists Work](#) .

- **Retention of SID history on tombstones.** The **sidHistory** attribute has been added to the set of attributes that are retained on an object tombstone when the object is deleted. If a tombstoned object is reactivated (undeleted), the **sidHistory** attribute is now restored with the object. For more information about tombstones, see [How the Data Store Works](#) .
- **Adprep.exe improvements for Windows 2000 Server upgrades.** The Adprep tool has been improved to reduce the impact of FRS synchronization that results from updating SYSVOL files during upgrade. Adprep is used to upgrade the Windows 2000 Server schema to the Windows Server 2003 schema and to update some forest- and domain-specific configuration, including SYSVOL, that is required for a Windows Server 2003 *domain controller* to be operational. The tool now allows performing SYSVOL operations in a separate step when the domain is prepared for upgrade. A new switch, **/gpprep**, has been added to accommodate the SYSVOL updates, which can be performed at a convenient time following the upgrade. The **adprep /domainprep** command, which formerly performed both directory and SYSVOL updates, now updates only the directory. Adprep also now detects third-party schema extensions that block an upgrade, identifies the blocking extensions, and recommends fixes. Microsoft Exchange schema objects are also detected so that the Exchange schema can be prepared appropriately to accommodate inetOrgPerson naming. For more information about Adprep.exe, see [Adprep](#) .
- **Improved authoritative restore.** The **authoritative restore** option in Ntdsutil now locates backlinks for all objects that are authoritatively restored, including links that were created before implementation of the Windows Server 2003 or Windows Server 2003 interim forest functional level, in which linked-value replication (LVR) functionality was introduced. For example, suppose that a user object is restored and the user belongs to group G1, which was created before the forest functional level was raised, and the user also belongs to group G2, which was created after the forest functional level was raised. During authoritative restore of the user object, the member attribute of G2 is updated, but not the member attribute of G1. Ntdsutil now creates a text file that identifies the authoritatively restored objects and uses this file to create an LDAP Data Interchange Format (LDIF) file that can be used to restore all backlinks for pre-LVR groups in this domain. In the example, when this LDIF file is run after authoritative restore, the restored user is added to group G1. A new option in **authoritative restore** also allows you to generate an LDIF file that you can use to restore links in other domains in which a restored object has backlinks.

## New Active Directory features in Windows Server 2003

With the new Active Directory® features available in Microsoft® Windows Server™ 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition, more efficient administration of the Active Directory directory service is available to you.

The following list summarizes the Active Directory features that are available by default on any *domain controller* running Windows Server 2003.

- **Multiple selection of user objects.** Modify common attributes of multiple user objects at one time.
- **Drag-and-drop functionality.** Move Active Directory objects from container to container by dragging one or more objects to a desired location in the domain hierarchy. You can also add objects to group membership lists by dragging one or more objects (including other group objects) to the target group.
- **Efficient search capabilities.** Search functionality is object-oriented and provides an efficient search that minimizes network traffic associated with browsing objects. For more information, see [Finding directory information](#) .
- **Saved queries.** Save commonly used search parameters for reuse in Active Directory Users and Computers. For more information, see [Using saved queries](#) .
- **Active Directory command-line tools.** Run new directory service commands for administration scenarios. For more information, see [Managing Active Directory from the command line](#) .
- **InetOrgPerson class.** The inetOrgPerson class has been added to the base schema as a security principal and can be used in the same manner as the user class. The userPassword attribute can also be used to set the account password. For more information, see [User and computer accounts](#) .
- **Application directory partitions.** Configure the replication scope for application-specific data among *domain controllers*. For example, you can control the replication scope of Domain Name System (DNS) zone data stored in Active Directory so that only specific *domain controllers* in the forest participate in DNS zone replication. For more information, see [Application directory partitions](#) .
- **Ability to add additional *domain controllers* using backup media.** Reduce the time it takes to add an additional *domain controller* in an existing domain by using backup media. For more information, see [Using the Active Directory Installation Wizard](#) .

- **Universal group membership caching.** Prevent the need to locate a global catalog across a WAN when logging on by storing universal group membership information on an authenticating *domain controller*. For more information, see [Global catalogs and sites](#) .
- **Secure LDAP traffic.** Active Directory administrative tools sign and encrypt all LDAP traffic by default. Signing LDAP traffic guarantees that the packaged data comes from a known source and that it has not been tampered with. For more information, see [Connecting to domain controllers running Windows 2000](#) .
- **Active Directory quotas.** Quotas can be specified in Active Directory to control the number of objects a user, group, or computer can own in a given directory partition. Domain Administrators and Enterprise Administrators are exempt from quotas.

### **New domain- and forest-wide Active Directory features**

New domain- or forest-wide Active Directory features can be enabled only when all *domain controllers* in a domain or forest are running Windows Server 2003 and the domain functionality or forest functionality has been set to Windows Server 2003. For more information about domain and forest functionality settings, see [Domain and forest functionality](#) .

The following list summarizes the domain- and forest-wide Active Directory features that can be enabled when either a domain or forest functional level has been raised to Windows Server 2003.

- **Domain controller rename tool.** Rename *domain controllers* without first demoting them. For more information, see [Renaming domain controllers](#) .
- **Domain rename.** Rename any Windows Server 2003 domain. You can change the NetBIOS name or DNS name of any child, parent, tree or forest root domain. For more information, see [Renaming domains](#) .
- **Different location option for user and computer accounts.** You can now redirect the default location for user accounts and computer accounts created by the following application programming interfaces (APIs): NetUserAdd, NetGroupAdd, and NetJoinDomain. You can redirect the location of the accounts from the Users and Computers containers to organizational units (OUs) where Group Policy settings can be applied. For more information, see [Redirect the Users and Computers Containers](#) .
- **Forest trusts.** Create a forest trust to extend two-way transitivity beyond the scope of a single forest to a second forest. For more information, see [Forest trusts](#) .
- **Forest restructuring.** Move existing domains to other locations in the domain

hierarchy. For more information, see [Renaming domains](#) .

- **Defunct schema objects.** Deactivate unnecessary classes or attributes from the schema. For more information, see [Deactivating a class or attribute](#) .
- **Dynamic auxiliary classes.** Provides support for dynamically linking auxiliary classes to individual objects, and not just to entire classes of objects. In addition, auxiliary classes that have been attached to an object instance can subsequently be removed from the instance.
- **Global catalog replication improvements.** Preserves the synchronization state of the global catalog when an administrative action results in an extension of the partial attribute set. This minimizes the replication traffic as a result of a partial attribute set extension by only transmitting attributes that were added. For more information, see [Global catalog replication](#) .
- **Replication enhancements.** Linked value replication allows individual group members to be replicated across the network instead of treating the entire group membership as a single unit of replication. For more information about linked value replication, see [How replication works](#) . In addition, new spanning tree algorithms make replication more efficient, as well as more scalable across a larger number of domains and sites in both Windows 2000 and Windows Server 2003 forests. For more information, see [Replication overview](#) .
- **User access control to resources between domains or forests.** Block users in a domain or forest from accessing resources in another domain or forest, and then allow selective access by setting the Allow to authenticate access control entry (ACE) on a local resource for the user or group object. For more information, see [Accessing resources across domains](#) or [Accessing resources across forests](#) .



## **LAMPIRAN O**

### **Top 10 Reasons to Install Windows Server 2003 SP2**

## Top 10 Reasons to Install Windows Server 2003 SP2

1

### **Security Updates/Hotfixes**

Windows Server 2003 SP2 will get all of your Windows Server 2003 and Windows XP Professional x64 Editions up to date with the latest Security Bulletin updates and Hotfixes, ensuring the highest level of security, reliability, stability, manageability, supportability and compatibility.

2

### **Deploy your operating systems more effectively**

Building upon our previous deployment solutions, Windows Deployment Services (WDS) offers customers a complete 'out of the box' provisioning solution. WDS provides organizations with manageable image store, remote booting, PXE boot support, and more; all in a greatly improved management interface. WDS also uses the new file-based Windows Imaging Format (WIM) which facilitates deployments on Windows Vista and Windows Server "Longhorn".

3

### **Improved networking performance**

Windows Server SP2 offers solutions to network traffic challenges in an era of the multi-Gigabit Ethernet. Increases to CPU resources required to handle high network traffic can potentially inhibit scaling and effectively reduce the performance gains that are possible with increased link speeds. Windows Server 2003 SP2 Scalable Networking Pack (SNP), introduces technologies that helps organizations cost-effectively scale network-based applications to meet growing demands. The Scalable Networking pack Increases network and application performance by freeing up CPU cycles and more efficiently using processor resources. More information on the Scalable Networking Pack can be found at [www.microsoft.com/snp](http://www.microsoft.com/snp).

4

### **Improved manageability for IPsec**

Server and Domain Isolation are key security benefits offered on Microsoft Networks. By using Active Directory, domain memberships and group policies, Server and Domain Isolation allows companies to logically segment their networks. This means that you can restrict non-domain computers which aren't managed at a corporate level (lab computers, guests or other unsecure systems) from communicating with non- domain

members. Service Pack 2 improves Server and Domain Isolation by reducing the IPsec filter set that needs to be managed from potentially hundreds of filters to as few as 2 filters. More information on Server and Domain Isolation can be found at [www.microsoft.com/sdisolation](http://www.microsoft.com/sdisolation).

### **5 Utility improvements**

Making common tasks easier, SP2 introduces customer-driven improvements to the Domain Controller Diagnostics tool (DCDIAG) and MS Configuration (MSCONFIG) tool. SP2 also has an updated Access Control List (ICACLS) program to allow for greater flexibility when backing up Access Control Lists.

### **6 Management tools made easier**

SP2 includes the Microsoft Management Console 3.0 (MMC 3.0). MMC provides a framework that unifies and simplifies day-to-day system management tasks on Windows by providing common navigation, menus, toolbars, and workflow across diverse tools. MMC tools (called snap-ins) can be used to administer networks, computers, services, applications and other system components. MMC does not perform administrative functions, but hosts a variety of Windows and non-Microsoft snap-ins that do.

### **7 Single install experience**

It patches both the R2 and non-R2 versions of Windows Server 2003. This reduces the amount of patch management for an organization.

### **8 Support for additional languages**

Service Pack 2 will be released in 9 additional localized languages for Windows Server 2003 x64 Editions including: German, French, Korean, Chinese Traditional, Chinese Simplified, Spanish, Italian, Russian and, Portuguese (Brazilian).

### **9 Performance improvements**

Service Pack 2 offers performance improvements for Windows Server 2003 running as a Virtual Server guest under high Advanced Processor Interrupt Controller (APIC) rates. It also improves SQL Server performance under intensive workloads. Both of these improvements lead to more efficient data process.



### **Connect to WPA2-protected wireless networks**

SP2 provides the ability to connect to wireless networks that are protected with Wi-Fi Protected Access 2 (WPA2). This allows server computers to use the highest level of wireless security that is based on current wireless standards.