Migrating from Windows NT4 to Server 2003
By Aloka Arachige & Peter Huddleson Catapult Integrated Systems © 2003

Introduction

This is a step-by-step guide for migrating from Windows NT 4 to Windows Server 2003. Included are procedures for the operating system (OS) upgrade and the NT domain to Active Directory (AD) migration. Also included are the procedures for configuration of multiple sites and Domain Controllers (DC) over a WAN connection.

Preparing the Primary Domain Controller for the Server 2003 Upgrade

- Start with the Primary Domain Controller (PDC) of the NT domain.

- Make sure the entire domain is synchronized so all the user and computer accounts exist on the PDC and all Backup Domain Controllers (BDC):
  - Go to Start, Programs, Administrative Tools, Server Manager.
  - Highlight the PDC and select Synchronize Entire Domain from the Computer menu.

- If you are using a BDC to perform the upgrade, you will first need to promote it to a PDC. (Note: Only perform this procedure if you wish to execute the upgrade and AD migration on the BDC while it is isolated from the NT domain. Otherwise, you will create a conflict with the original PDC once you promote the BDC):
  - Go to Start, Programs, Administrative Tools, Server Manager.
  - Highlight the BDC you wish to promote from the list of computer accounts and then select Promote to Primary Domain Controller from the Computer menu.

- Define the PDC as its own primary DNS and WINS servers. Part of the migration process to AD includes the installation and configuration of DNS on the master AD Domain Controller (DC). This process goes more smoothly if the PDC already has itself listed as the primary DNS server, even if DNS is not currently installed on it. Similarly, by having the PDC defined as its own WINS server, the process of installing WINS and migrating other machines from the NT domain to AD will go more smoothly. More detail about the installation and configuration of DNS and WINS will come later in this document. For now, simply input the IP address of the PDC as the primary DNS and WINS servers:
  - Right click on Network Neighborhood and select Properties.
  - Click on the Protocols tab.
  - Highlight TCP/IP Protocol and hit the Properties button.
  - Click on the DNS tab, click on the Add button, type in the IP address of the PDC and click Add.
  - Highlight all other DNS servers in the DNS Service Search Order window and click Remove until only the PDC is listed.
  - Click on the WINS Address tab, type in the IP address of the PDC in the Primary WINS Server field and remove any other WINS server that may be defined in the Secondary WINS Server field.
  - Click OK and then Close.
  - Click Yes to restart your computer when prompted.

- The PDC is now ready to be upgraded to Windows 2003 Server:
  - Insert the Windows Server 2003 CD into the PDC.
  - When the menu appears, select Install Windows Server 2003.
  - In the Installation Type field, make sure Upgrade (Recommended) is displayed and click Next.
  - Select I accept this agreement and click Next.
  - Input the Product key in the appropriate fields and click Next.
  - Since this is an upgrade from Windows NT, a Report System Compatibility window will display to provide information about which client operating systems are not compatible with Windows Server 2003. To view information about this incompatibility, click Details. When finished, click OK to close the Details window and then click Next to continue the upgrade.
  - The installer will now copy the installation files and reboot the computer automatically.
o Allow the computer to boot up on its own. (DO NOT press any key to boot from CD or select another boot option other then Windows Server 2003 Installation from the boot menu.)

o The installer will continue the installation process. This will take approximately 45 minutes to complete, depending on your hardware.

o The computer will reboot again as part of the installation. Again, allow the computer to boot up on its own by not hitting any keys.

o When the installation is finished, the computer will reboot a final time. Again, allow it to come up on its own.

Installing Active Directory and DNS on the Primary DC

- Now it is time to install AD and DNS on the newly upgraded DC. After it comes back up from the final installation reboot, it will display an Active Directory Installation Wizard window:
  
  o Click Next on the Welcome to the Active Directory Installation Wizard window.
  
  o Click Next on the Operating System Compatibility window.
  
  o Select Domain in a new forest on the Create New Domain window. This is the option to use for the first domain controller in the AD. Click Next.
  
  o In the New Domain Name window, type the fully qualified domain name in the Full DNS name for the new domain field (e.g. company-ad.company.com). Click Next.

  Note: It is strongly recommended that you make your AD domain a sub domain of your second-level (company) domain. The reason for this is because the DNS zones on your second-level domain name are most likely managed by your ISP. If you use this level of DNS naming, then your internal (Windows) DNS zones will overlap the zones on the publicly available DNS servers your ISP is using to manage your domain name. This will cause DNS resolution between your public and private servers to not work correctly. You could make your Windows-based DNS servers the primary, public-facing DNS servers, which would allow you to use a second-level domain name on the DC. This is not advisable, however, since you would be exposing your entire AD structure to the open Internet, creating a major security hole. Hackers could use a process called “dig” to gather information about your Windows network through publicly-exposed Windows-based DNS. Our purpose in using Windows-based DNS with AD is simply to implement a method for AD clients and servers to register and resolve host names and IP addresses on a private network.

  o In the Forest Functional Level window, select Windows 2000. This is the most compatible option for non-native Server 2003 AD implementations. Click Next.
  
  o Select both default entries in the Database and Log Folders window (i.e. C:\WINNT\NTDS). Click Next.
  
  o Again, select the default entry in the Shared System Volume window (i.e. C:\WINNT\SYSVOL). Click Next.
  
  o In the DNS Registration Diagnostics windows, select Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server. This is extremely important when setting up the first domain controller since this is how it links to Windows-based DNS. Click Next.
  
  o Select Permissions compatible with pre-Windows 2000 server operating systems in the Permissions window. This gives you compatibility with any existing NT domain clients. Click Next.
  
  o Type the domain administrator’s password in the two fields in the Directory Services Restore Mode Administrator Password window. Click Next.
  
  o Click Next in the Summary window to execute the AD installation. This process will take about 5-10 minutes to complete.
  
  o When the installation completes, click Finish in the Completing the Active Directory Installation Wizard window. Then click Restart Now to reboot the server.

- When the DC comes back up, you will need to configure DNS:
  
  o Click on Don’t display this page at logon in the Manage Your Server window and close the window.
  
  o Go to Start, Programs, Administrative Tools, DNS. This will start the DNS management console.
  
  o Expand the folder list under the DNS object. Keep expanding it until you see the Forward Lookup Zones and Reverse Lookup Zones folders. Initially, there will be two Forward zones and no
Reverse zones defined. **Note**: It is very important that you do not remove either of the forward zones. They are both necessary for the process of migrating servers and clients from the NT domain to AD.

- Right-click on the **Reverse Lookup Zones** folder and select **New Zone**.
- Click **Next** on the **Welcome to the New Zone Wizard**.
- Select **Primary Zone** on the **Zone Type** window. Click **Next**.
- In the **Active directory Zone Replication Scope**, select **To all domain controllers in the Active Directory domain company-ad.company.com**. Click **Next**.
- Enter the network portion of the DC’s IP address in the **Network ID** field on the **Reverse Lookup Zone Name** window. (e.g. If its address is 192.168.1.100 /24, enter 192.168.1) Click **Next**.
- In the **Dynamic Update** window, select **Allow only secure dynamic updates (recommended by Active Directory)**. Click **Next**.
- Click **Finish** to complete the wizard.
- You should now see a folder under **Reverse Lookup Zones** called **192.168.1.x Subnet**.

- **Now that DNS has been configured, there are a few more steps to make the server fully functional:**
  - Call up a DOS command prompt (**Start**, **Run**, **cmd**) and type the following command:
    ```
    net time /setsntp:ntp.timeserver.com
    (ntp.timeserver.com is the host name or IP address of an Internet time server)
    ```
  - This will synchronize the clock on the AD controller and is necessary for its proper functioning. Type **exit** to close the command window.
  - Go to **Start**, **Run**, **Administrative Tools**, **Event Viewer**. Highlight each of the six items in the left pane, right click and select **Clear All Events**. When prompted to save the entries, select **No**. Because AD installation creates a number of error messages, it is a good idea to clear the error logs before the server is rebooted so you can clearly see if there are any remaining issues.
  - Reboot the server. After the server comes back up, check the Event Viewer again to make sure there are no errors.

- **Make sure the correct DNS server is listed:**
  - Right click on **My Network Places** and select **Properties**.
  - Right click on the **Local Area Connection** icon and select **Properties**.
  - Highlight **Internet Protocol (TCP/IP)** and hit the **Properties** button.
  - Click on the **Advanced** button, then on the **DNS** tab. Make sure 127.0.0.1 is not listed.
  - If it is, highlight it and click **Remove**. The only IP address that should be listed is that of the primary DC.
  - Click **OK** on the next three windows to close them, and then close the **Network Connections** window.

- **Install WINS (if not already installed):**
  - Go to **Start**, **Settings**, **Control Panel**, **Add or Remove Programs**, then click on **Add/Remove Windows Components**.
  - Double-click **Networking Services** and select **Windows Internet Name Service (WINS)**. Then click **OK** and **Next** (make sure you have the Windows Server 2003 media in the CD-ROM or that the i386 directory is staged on the server’s hard drive).
  - Click **Finish** and reboot if prompted.
  - Double check to make sure the primary DC is configured to use itself for WINS resolution.

- **Check WINS registrations:**
  - Go to **Start**, **Programs**, **Administrative Tools**, **WINS**.
  - Highlight **Active Registrations**, right-click and select **Display Records**.
  - Check **Filter Records matching this Name pattern** and type a * in the field.
  - Make sure the primary DC’s name and IP address registered.
Preparing the Active Directory for Additional Domain Controllers

- Create a new site to contain a remote DC:
  - Go to Start, Programs, Administrative Tools, Active Directory Sites and Services
  - Expand Sites
  - Highlight Sites, right-click and select New Site.
  - Type a name for the new site in the Name field (e.g. Remote-Site). Then highlight DEFAULTIPSITELINK and click OK. This creates a new site for the remote DC, which we will discuss in the next section of this document.
  - Click OK in the AD message window.

- Now we need to link the original site (Default-First-Site-Name) and the new site (Remote-Site) to their respective subnets:
  - Right-click Subnets and select New Subnet.
  - Type the network address of the primary DC in the Address field (e.g. if IP address is 192.168.1.100, then network address is 192.168.1.0).
  - Type the corresponding subnet mask of the primary DC in the Mask field (e.g. the above IP address would have a subnet mask of 255.255.255.0).
  - Highlight Default-First-Site-Name and click OK.
  - Repeat the above steps to create a subnet for the Remote-Site site. The only difference is that you will be inputting a different network address and linking it to Remote-Site.

Installing and Configuring Server 2003 on the Remote Server

The process for installing and configuring the remote DC is similar to what's already been done for the primary DC at the main site. The one major difference is that we will be installing the remote DC as a new 2003 server rather than as an upgraded NT server. Other differences will be highlighted as they come up.

- For this part of the procedure, we will do a clean installation of Windows Server 2003 on a new machine:
  - Boot the remote server using the Windows Server 2003 CD. This will begin the installation wizard.
  - Hit Enter at the Setup Notification screen.
  - Hit Enter at the Welcome to Setup screen.
  - Hit F8 to agree to the licensing agreement.
  - Hit Enter to begin installation on an existing partition. (If there is no partition defined, hit C to create a new one. Enter the size of the new partition in MB and hit Enter. Hit Enter again to begin the installation onto the new partition.)
  - Select Format the partition using the NTFS file system <Quick> and hit Enter.
  - The installer will now format the new partition and copy the files needed for installation to the hard drive. This process will take several minutes depending upon the speed of your server and size of the partition. When it is finished, it will reboot automatically. Be sure not to hit any keys so that it will boot up using the new partition.
  - Once back up, the server will begin the graphical part of the installation. Much of this is automatic, but there will be a few places for user input, noted below. This part of the installation will take an additional 30-45 minutes.
  - Click Next on the Regional and Language Options window.
  - Type in a Name and Organization in the corresponding fields on the Personalize Your Software window and click Next.
  - Input the Product key in the appropriate fields and click Next.
  - Select the Licensing Mode you wish to use and click Next.
  - Enter the Computer name and Administrator password in the appropriate fields and click Next. If the Windows Setup message screen warns you about your password, click No to change it or Yes keep it.
  - On the Data and Time Settings window, verify that the information is correct and click Next.
Select Custom Settings on the Network Settings window and click Next. This is necessary because we are installing a server which will become a domain controller and DNS server, both of which require a static IP address.

1) On the Networking Components window, verify the listed device is the one you want to configure. If not, hit Next until it is listed. Then, highlight Internet Protocol (TCP/IP) and hit the Properties button.

2) On the TCP/IP Properties window, select Use the following IP address and input the server’s IP address, Subnet mask and Default gateway in the appropriate fields. Note: Make sure this IP address corresponds to the new subnet you created in the previous section for Remote-Site.

3) Select Use the following DNS server addresses and input the IP address of the primary domain controller previously configured.

4) Click on the Advanced button, and then on the WINS tab. Click on Add, input the IP address of the primary domain controller and then click the second Add button.

5) Select Enable NetBIOS over TCP/IP and click OK.

6) Click OK again to exit the TCP/IP Properties window. Then click Next.

In the Workgroup or Computer Domain window, select the first option (No, this computer is not on a network…) and type in a name for the workgroup (e.g. GROUPNAME-WG). This setting will be changed later when the server joins the AD domain. For now, though, it needs to be in workgroup mode. Click Next.

The installation will now continue automatically to completion, when it will reboot itself.

As before, click on Don’t display this page at logon in the Manage Your Server window and close the window.

Once the basic Windows Server 2003 installation is done, it is time to join the new server to the existing Active Directory created previously.

Right-click on My Computer and select Properties.

Click the Computer Name tab and then on the Change… button.

In the Member of section, click the Domain option and type the name of the previously defined AD domain (e.g. company-ad.company.com). Click OK.

Type in the name of a user account (usually, administrator) which has rights to join computers to the domain and input the corresponding password. Click OK.

After a few moments, you should see a confirmation that the computer is now a member of the AD domain (e.g. “Welcome to the company-ad.company.com domain”). Click OK.

You will be prompted to reboot the computer. Click OK to close the message window and then click OK again on the System Properties window.

Click Yes to reboot the computer. Do not be concerned if the server seems to take a long time to boot up after joining the AD domain. This is common when a machine is first joined to a domain.

Verify that the remote server is now in the AD:

On the primary DC, go to Start, Programs, Administrative Tools, Active Directory Users and Computers.

Click on the Computers object and verify that the remote server is listed.

Double-click on it to open its properties. Verify that its full name is listed in the DNS name field (e.g. remote-dc.company-ad.company.com).

Promoting the Remote Server to be a Domain Controller

After the computer comes back up from joining the domain, it is time to promote it to an AD domain controller. This will be similar to the procedure outlined in the Installing Active Directory and DNS on the Primary DC section, except that you must start this process manually (Note: DNS will not install automatically during this process since it will detect the DNS server on the other DC.):

On the remote server, log on to the AD as the domain administrator. (Be sure you are logging into correct domain in the Log on to field.) Again, do not be concerned if the server seems to take a long time to login.

Go to Start, Run and type cmd in the Open field to start a command window.

Type dcpromo and hit Enter to begin the Active Directory Installation Wizard. Click Next.

Click Next on the Operating System Compatibility window.
On the Domain Controller Type window, select Additional domain controller for an existing domain and click Next.

On the Network Credentials window, type in administrator and its corresponding password in the User name and Password fields. The Domain field should already have the fully qualified domain name for the administrator user displayed (e.g. company-ad.company.com). Click Next.

On the Additional Domain Controller window, type in the fully qualified domain name in the Domain name field for the domain you are adding the DC to. In this case, it is the same as that in the above step and should already be filled-in. Click Next.

Select both default entries in the Database and Log Folders window (i.e. C:\WINDOWS\NTDS). Click Next.

On the Shared System Volume window, type in the fully qualified domain name in the Domain name field for the domain you are adding the DC to. In this case, it is the same as that in the above step and should already be filled-in. Click Next.

Type the domain administrator password in the Restore Mode Password and Confirm Password field on the Directory Services Restore Mode Administrator Password window. Click Next.

Click Next on the Summary window to begin the DC promotion. This process will take several minutes to complete.

Once the wizard completes, click Finish on the Completing the Active Directory Installation Wizard window.

Click the Restart Now button to reboot the server.

On the primary DC, go to Start, Programs, Administrative Tools, Active Directory Users and Computers.

Click on the Domain Controllers object and verify that the remote server is listed.

Configure the remote DC in the AD Sites and Services:

After the remote server comes back up from its AD promotion, go to Active Directory Sites and Services on the primary DC and expand the Remote-Site site. The remote DC should now be listed under this new site.

Expand Default-First-Site-Name completely.

1) Right-click on NTDS Settings in the left pane and select Properties.
2) On the General tab, check the Global Catalog box (if not already checked) and select Default Query Policy in the Query Policy field.
3) On the Connections tab, verify that the remote DC is listed in both the Replicate From and Replicate To fields.
4) Click Apply and then OK to close the window.
5) Highlight NTDS Settings in the left pane.
6) In the right pane, right-click on the displayed object (e.g. <automatically generated> SERVER-REMOTE Remote-Site Connection) and select Replicate Now. Click OK on the Replicate Now message window.

Repeat the above steps for the remote site. Click the Refresh button and then expand Remote-Site completely.

1) Right-click on NTDS Settings in the left pane and select Properties.
2) On the General tab, check the Global Catalog box (if not already checked) and select Default Query Policy in the Query Policy field.
3) On the Connections tab, verify that the primary DC is listed in both the Replicate From and Replicate To fields.
4) Click Apply and then OK to close the window.
5) Highlight NTDS Settings in the left pane.
6) In the right pane, right-click on the displayed object (e.g. <automatically generated> PRIMARY-SERVER Default-First-Site-Name Connection) and select Replicate Now. Click OK on the Replicate Now message window.

The two DCs are now both Global Catalog servers and are able to replicate to each other.
**Final Steps**

- Install and Configure DNS and WINS on the remote DC:
  - Go to *Start, Settings, Control Panel, Add or Remove Programs*, then click on *Add/Remove Windows Components*
  - Double-click *Networking Services* and select *Domain Name System (DNS)* and *Windows Internet Name Service (WINS)*. Then click *OK* and *Next* (make sure you have the Windows Server 2003 media in the CD-ROM or that the i386 directory is staged on the server’s hard drive).
  - Click *Finish* on the *Completing the Windows Components Wizard* window.
  - Configure the remote DC to use itself for primary DNS and WINS resolution, and the primary DC for secondary DNS and WINS resolution.
  - Reboot both the primary and remote domain controllers.

- Check to make sure all the DNS entries from the primary server replicated properly to the remote server. You should see matching entries on both the forward and reverse zones on both servers. It may take up to 15 minutes and several reboots before all the DNS entries are replicated on both domain controllers.