Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Active Directory: Disaster Recovery Steps

Jeffrey Palgon
GSEC 1.4 – Option 1

Introduction

Ask most any company's management what their most critical data is and you are likely to get the common responses of a marketing database or client files. While these are important, an organization's Active Directory database is often overlooked. In the event of a disaster, it would be rather complicated to access a marketing database when there are no logon servers available to authenticate yourself and your credentials. Since policy usually reflects management's intentions, odds are pretty good that most organizations do not have a Disaster Recovery policy that outlines the steps required to preserve the Active Directory database.

This document is intended to demonstrate the steps required to backup and authoritatively restore an Active Directory structure in the potential event of a disaster. In this tutorial, we have only used the Windows 2000 Server software and its integrated tools to demonstrate the low cost involved with this process. Following these simple steps can be the difference between restoring a Domain Controller in a few days to a few hours.

What is Active Directory?

Active Directory is a transactional database containing all users, groups, and computer objects belonging to a domain. In addition to these accounts, organizational units may be created to group common users together based on organizational structure. Group policies may be used to distribute security settings, workstation settings, and even automatic software installation packages.

Active Directory resides on all Windows 2000 Domain Controllers. Perhaps some of Active Directory's most important functions are authentication and authorization. In addition, Active Directory can also store the organization's DNS records.

Authoritative Restore vs. Non-Authoritative Restore

When restoring our Active Directory, we have two methods to pick from: Authoritative and Non-Authoritative restores. To put it simply, every time a change is made to the Active Directory database, an Update Sequence Number (USN) of the database is increased by one. When all of the Domain Controllers poll each other for replication of the database, they will use the database with the highest USN.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Supposing we had several Domain Controllers, if one of them failed and we were forced to rebuild it, we would choose to restore it non-authoritatively. We would restore Active Directory in Non-Authoritative mode with the most recent backup for that specific server. After the restore completes, the rebuilt server will have the USN at the time of the last backup. Given that many changes have happened on the other Domain Controllers since the time of the last backup, the rebuilt server will poll the other servers for the most recent copy of the Active Directory database. From then on, all Domain Controllers will be up to date.

An Authoritative Restore should only be performed if an administrator deleted a large amount of the Active Directory database, or in the event that all Domain Controllers fail or are destroyed. The Active Directory database will be restored and in the process the USN for this database will be increased by a very large number. This tells all other Domain Controllers that they should replicate with this server for the most recent version of Active Directory. Authoritative Restores should only be performed on the first Domain Controller to be restored. All subsequent restores of Domain Controllers should be performed non-authoritatively.

Active Directory Disaster Recovery Overview

Our first step in creating a disaster recovery plan for our Active Directory is to backup the Active Directory database. Since Active Directory resides on all Windows 2000 Domain Controllers, we must backup all of our Windows 2000 Domain Controllers in their entirety.

Once we have our backups of our servers, we must replicate our backups to a centralized backup server to add an extra layer of prevention, similar to a defense-in-depth strategy. This way, if our Domain Controller fails, we have a copy locally on a centralized backup server. To prevent against eavesdropping or interception and to provide encryption, the replication between the servers should be conducted over a line using an IPSEC connection. After our backups have been replicated, the next step would be to transfer the backups to removable media to be stored off-site.

Next, we will assume that an event has occurred completely destroying our network. First, we will reinstall Windows 2000 on a new server. Then, we will begin the authoritative restoration process of our Active Directory and Domain Controllers. Finally, we will verify that our Active Directory restore is fully operational.

Test Environment Setup

Figure 1 shows our test environment configuration.

- Yoda – Windows 2000 Domain Controller with DNS-integrated Active Directory

© SANS Institute 2003, Author retains full rights.

- Obiwon – Windows 2000 Backup Server
- An IPSEC connection between the Domain Controller and the Backup Server
- Software used:
  - Windows 2000 Advanced Server
  - Robocopy

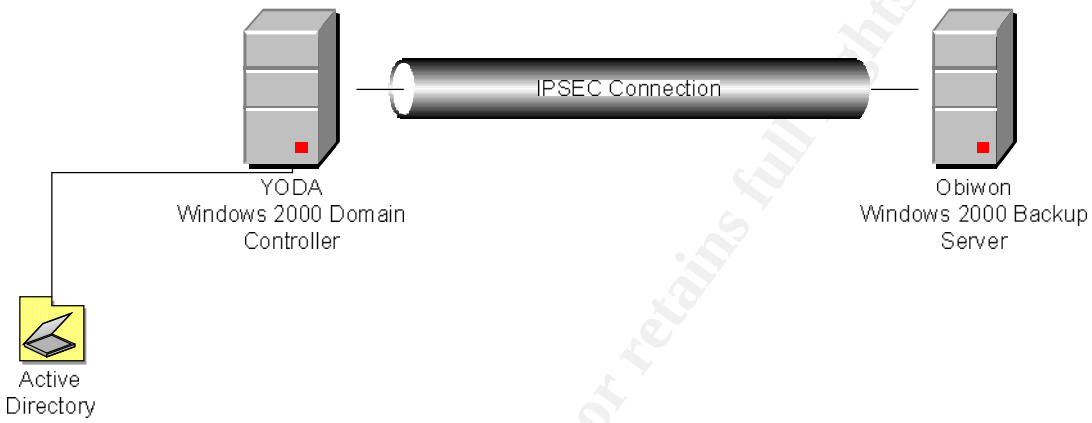
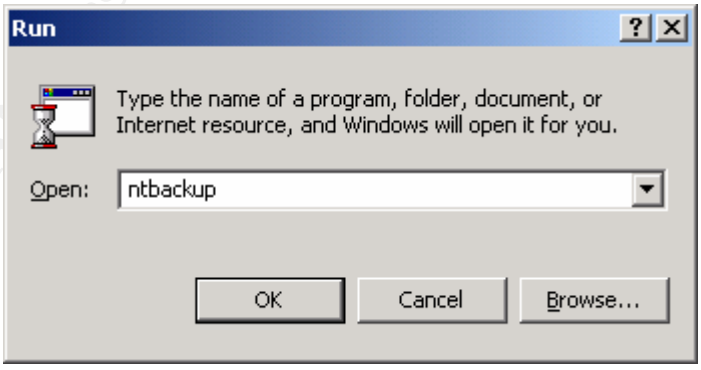


Figure 1

© SANS Institute 2003, Author retains full rights.

Creation of Backups

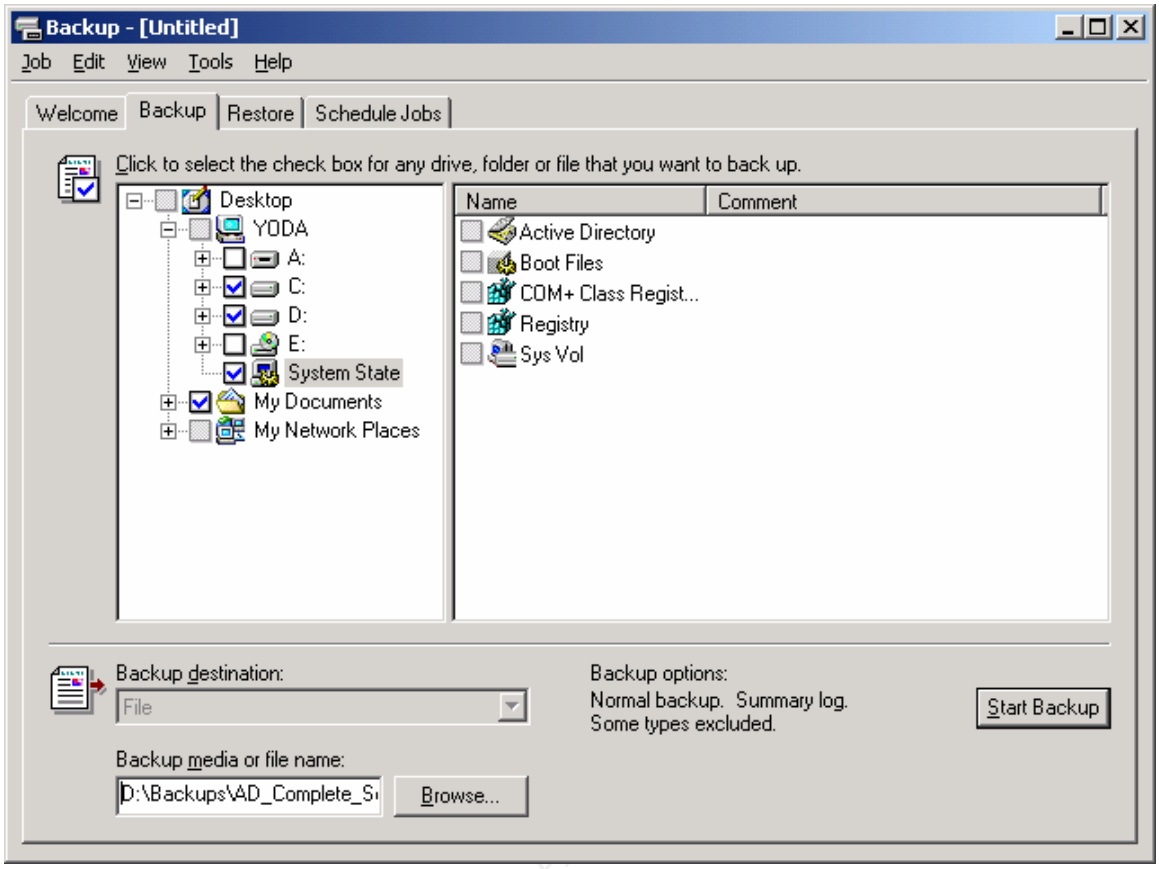
The first step in our Disaster Recovery Program is to make a backup set of our Active Directory. We begin by logging onto the Domain Controller that we wish to backup as a user belonging to the *Administrators* or *Backup Operators* group. From there, we click **Start → Run…**, then type **NTBACKUP** and click **OK**.



You will be presented with a window welcoming you to the Windows 2000 Backup and Recovery tools.

To create the backup set, click the **Backup** tab.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



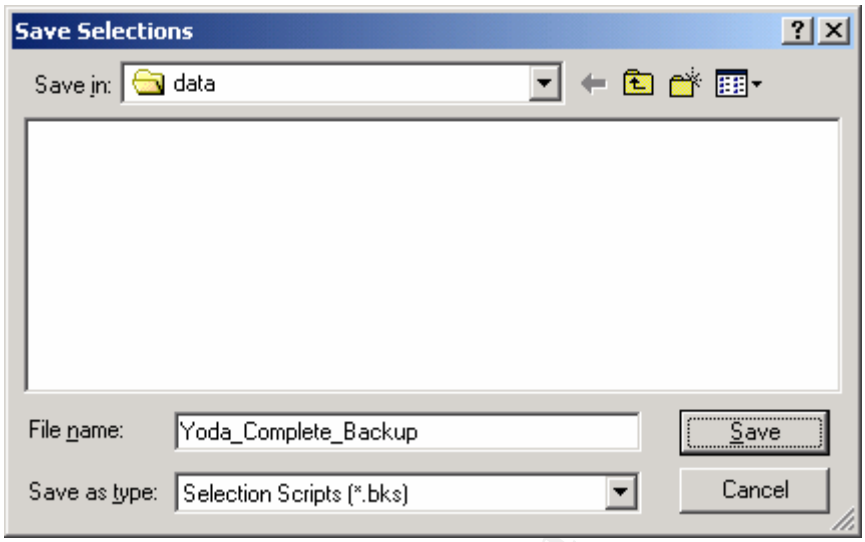
In order for us to make a complete backup set, we must select the System State. In this screen capture, the System State selection is highlighted to show the components to be backed up: Active Directory, Boot Files, COM+ Components, Registry, and SysVol. Notice that you cannot select Active Directory individually, as the other components must be included as well. When we backup Active Directory, the database (Ntds.dit), the checkpoint file (Edb.chk), and all of the transaction logs are backed up. When we backup SysVol, we are backing up all logon scripts that you may be using as well as all Group Policies.

Next, we must select to backup all local drives. This is the most common pitfall in backing up Active Directory. If we did not backup the local drives, we would not be able to completely restore our Domain Controller to the way it was before. For instance, if we did not backup the local drives of our server and instead chose to only backup the System State, then we would have to bring the server back to Service Pack that it was on at the time of the backup before we can restore our Active Directory. Any security patches that were on the server at the time of the backup would need to be added as well. This could be a tedious and lengthy process that has the potential for many errors. It is for these reasons that we choose to backup the entire server.

In the lower-left, enter the Backup file name. Here, we have directed the file to save under a Backup folder on our D drive.

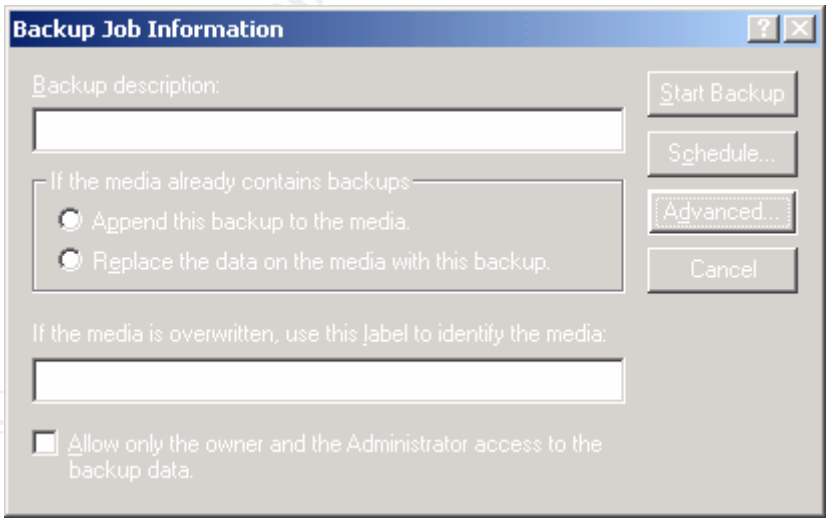
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Next, we must save our selections to reuse in the future. Click **Job → Save Selections As…**.



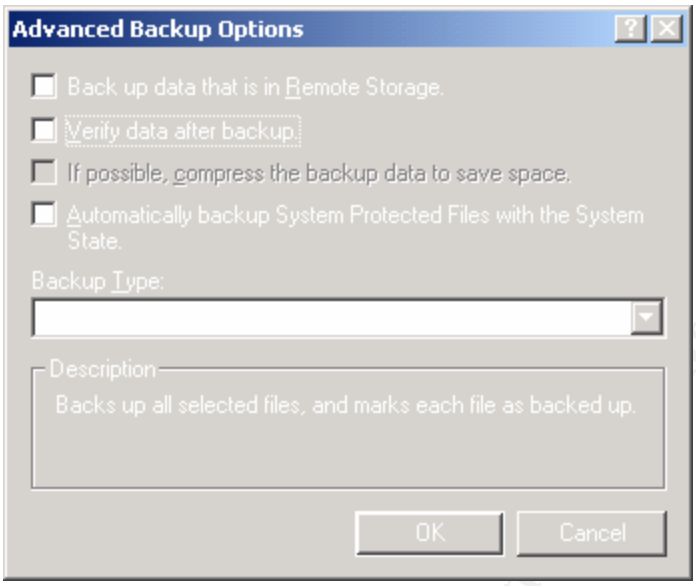
Enter the File name you wish to use and click **Save**. Be sure to choose a descriptive name for the backup that includes the server name. We will be replicating this backup to the central backup server where there is potential to be several other backups and this naming will help us differentiate them quickly.

You will be returned to the main backup screen. Click **Start Backup** to begin scheduling the backups and to create advanced options.



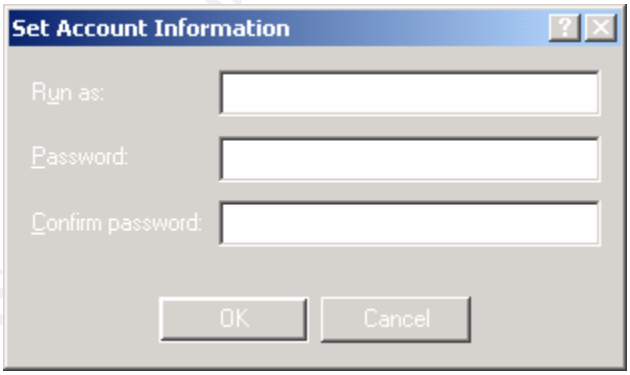
Click **Advanced…**.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



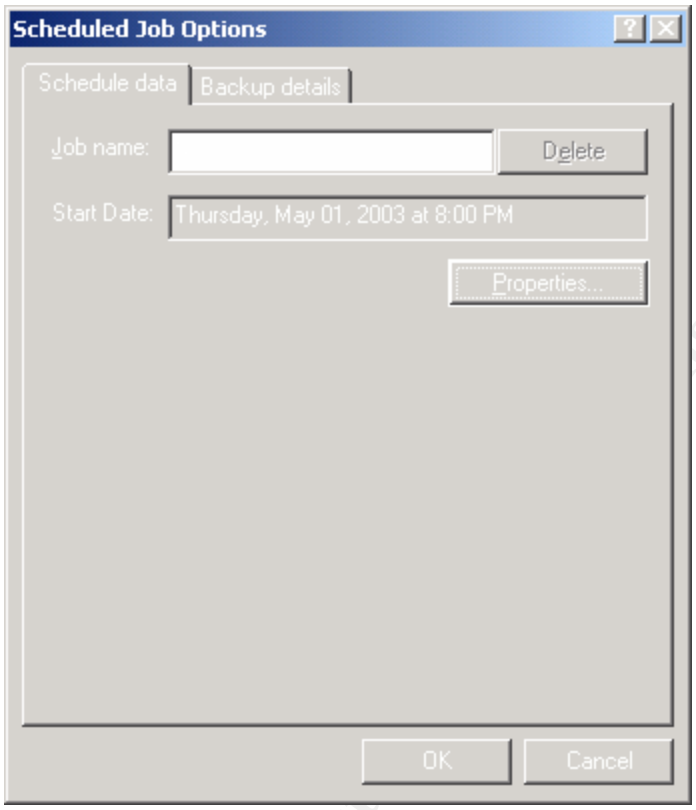
Here, we have selected to verify the data after it is backed up. This will verify that the data was backed up correctly and will minimize the possibility that the data will be corrupt upon restoration. Also we have selected the Backup Type to *Normal*. All backups of Active Directory should be Normal, or Full. Active Directory will not be able to authoritatively restore itself it the backup has been created any other way (Copy, Differential, Incremental, etc.). When finished, click **OK**.

Next, we will schedule the backup to occur at a certain time. Click **Schedule…**.



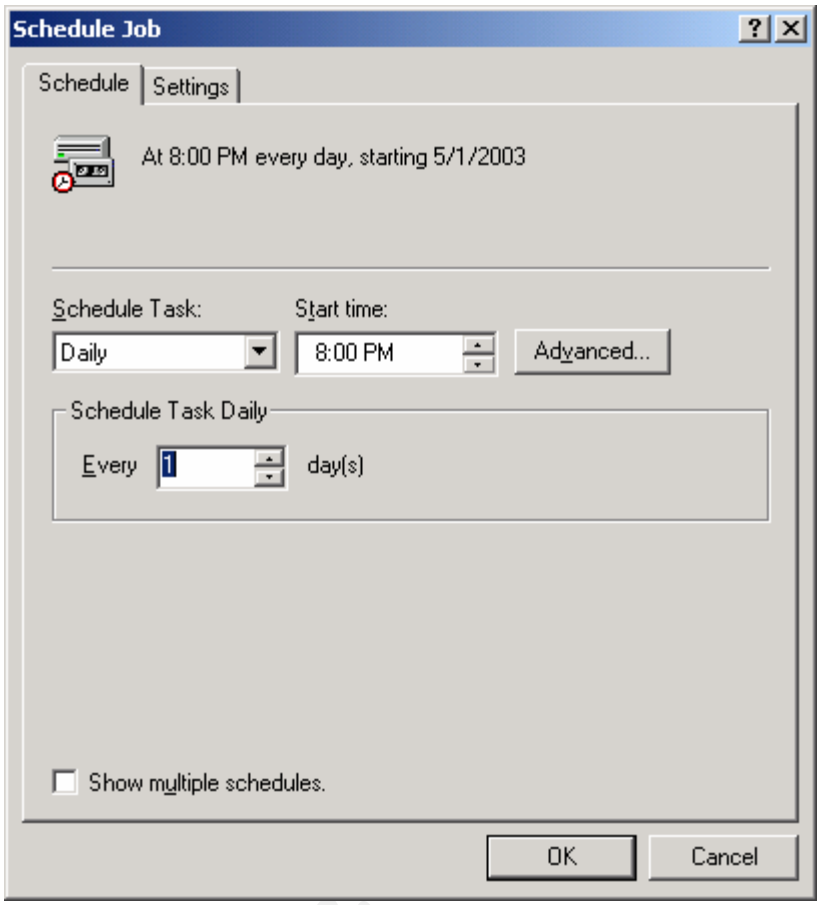
In the *Run as:* line, insert the name of a domain account that will be used to backup the file in the format of *DOMAINNAME\USERNAME*. In this example, we used an account called "BackupServices" on the JEDI domain. This account is only used for running backups for our backup software and cannot be used to log onto other machines. The only group this account belongs to is the *Backup Operators* group, giving it the minimal rights needed to backup our server. This account's information should be kept secret and the password should be long and complex. Next enter the password twice for the account. Click **OK**.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Enter a descriptive name for the job, and click **Properties…**.

© SANS Institute 2003, Author retains full rights.

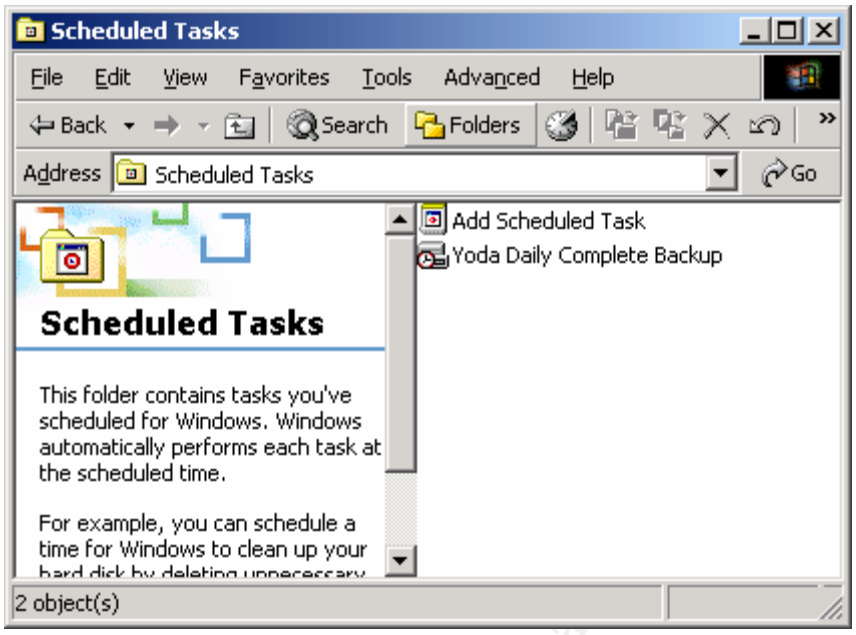


It is recommended that you backup your Active Directory and Domain Controllers daily. It is understood that the benefits of daily backups are difficult to prove to management, and therefore you may be backing up your Active Directory with less frequency. Remember that due to the tombstone life of Active Directory objects, all Active Directory backups have a 60-day shelf life. At a minimum, we must backup our Active Directory every 60 days or less. It is obviously not recommended that you wait the maximum to run the backup, as potentially you would have to recreate up to 60 days of user accounts, groups, and group policies.

We have scheduled our backup to start today at 8:00 PM and to repeat every day of the week. Click **OK** twice to continue.

To finally set our backup to begin, click **Start Backup**. The backup will now be scheduled to run at the time you have set. To verify this, click **Start → Settings… → Control Panel → Scheduled Tasks**. In this window, you will see your new backup job scheduled.

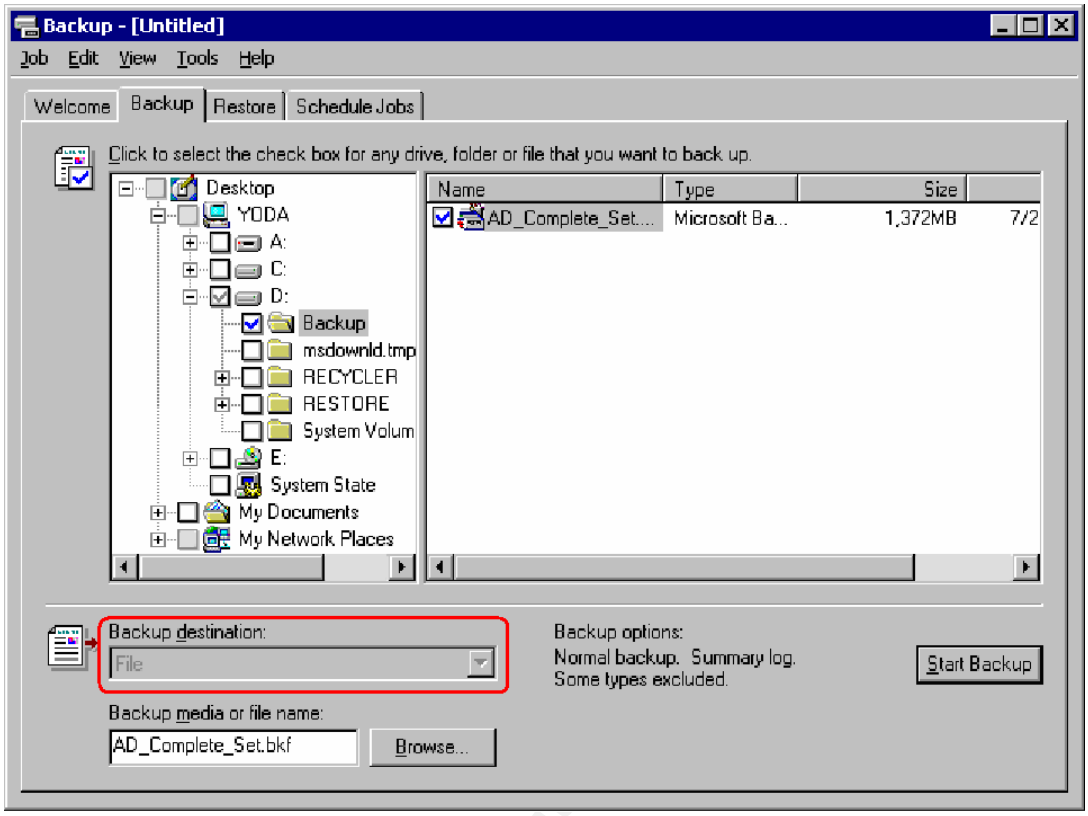
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



You can check the backup folder after the job is completed to see the backup file has been created. Now that we have successfully backed up our server, the next step is to get the backup file onto password-protected removable media so that it can be stored off-site.

To do this follow the steps we just went through in backing up Active Directory. The only differences will be that instead of backing up all the local drives and the System State we will backup the backup file we created. In our example, the file is located at *D:\Backup\AD_Complete_Set.bkf*.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



The next change will be to copy the file to removable media instead of to disk. Under the *Backup destination*, select *Removable Storage*. In our example, we did not have the luxury of a tape drive, but where you would select the tape drive has been highlighted. Again, follow the steps to schedule that backup to run automatically. In most situations, you will most likely being using third-party backup software for this operation. It is advised that you select to password-protect this media if at all possible.

Redundancy through Replication

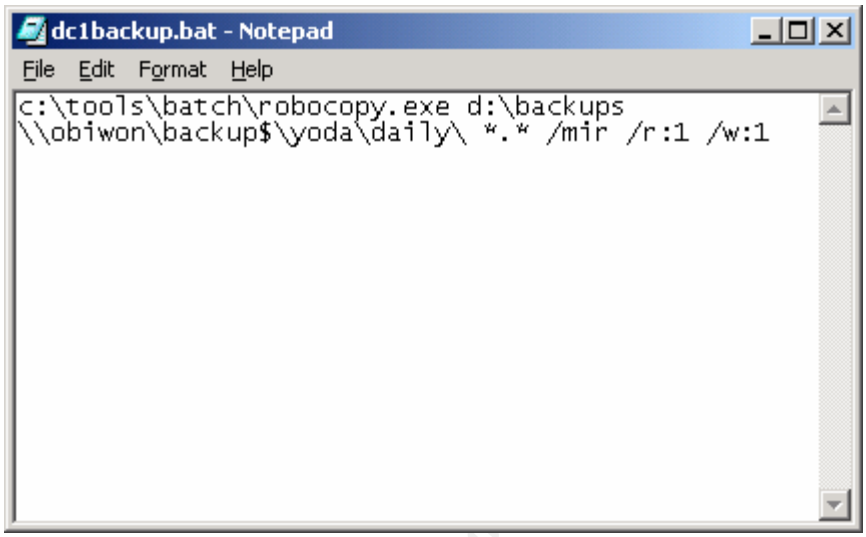
To provide for redundancy and an additional layer of protection, the backup file should be copied to a backup server. It is suggested that you have a centralized backup server on your network. Then you can have all of your server's backups located in one place. From there, you would copy the backups onto your removable media and store them off-site.

We will use a free tool called Robocopy to automatically copy the backup file we just created to a central backup server. Robocopy is a free tool that can be found on the Windows 2000 Server Resource Kit. Copy robocopy.exe to a folder on your server. We chose to install it to *C:\Tools\Batch\Robocopy.exe*.

From here, we will create a batch file to tell Robocopy what to backup and how to do it. First, open up Notepad by clicking **Start → Run → Notepad**. Start by typing the path to the robocopy.exe file, *C:\tools\batch\robocopy.exe*. Next specify the path to what it is

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

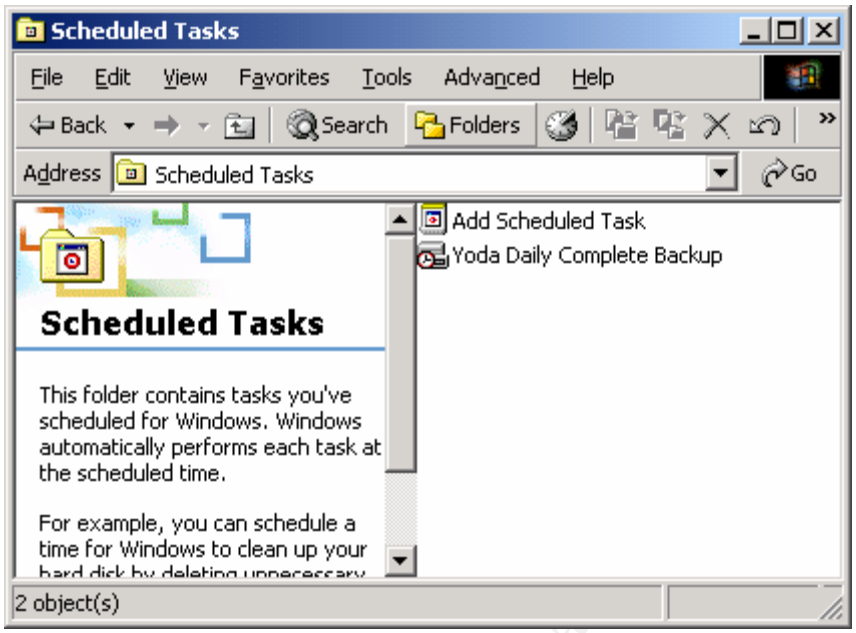
you are going to backup. Remember, we had our backups saved at *D:\backups*. We could insert a file name here, but we chose to backup the folder just in case there are multiple versions residing in this folder. Next, enter the UNC path of the backup server, the folder you wish to save the backup to, and any necessary program switches. Last, save the file using the *.bat* file extension.



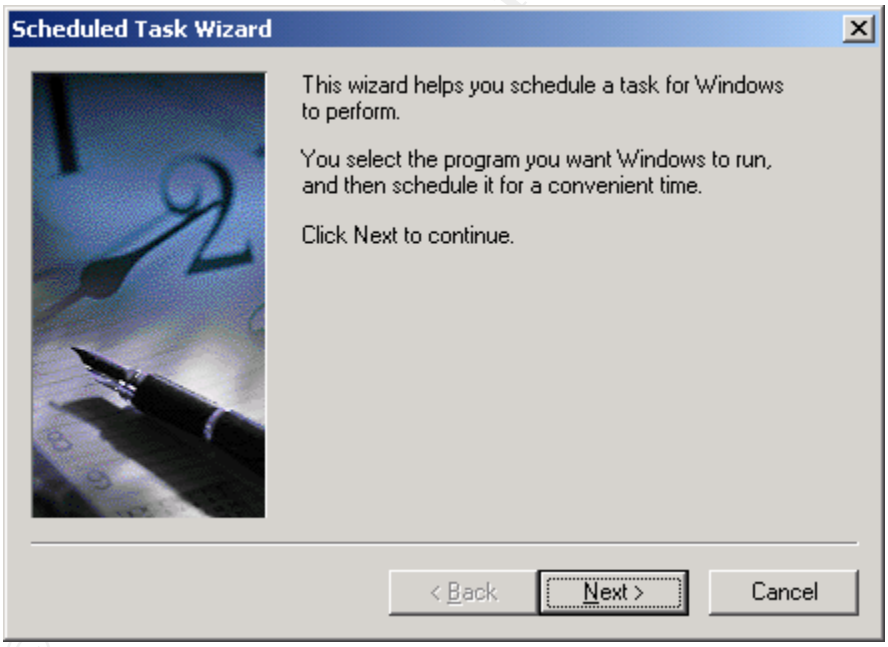
In our example, OBIWON is our backup server, so we enter *\\obiwon\backup$\yoda\daily\ *.* /mir /r:1 /w:1*. The "*.*" is used to copy all files that reside in the *D:\backups* folder. The "/mir" switch tells Robocopy to make a perfect mirrored copy of the directory tree, while the "/r:1" switch tells Robocopy to retry copying the file 1 time if it has a problem copying and "/w:1" tells Robocopy to wait 1 second before retrying. If you do not enter in numeric values for Robocopy to retry and/or wait, then the default settings will be enforced. Robocopy's default retry amount is one million retries and the default wait time is 30 seconds. If this were to extend out to the maximum time, it would take approximately 347 days. Prior experience shows that if Robocopy has a hard time copying a file, then it will continue to have a hard time copying the file. You may be disappointed to come in the next day to find that your backup did not run because Robocopy was hung up trying to copy a file. It is for this reason that we suggest you specify a reasonable retry amount and wait period.

Now that we have created our script, we must schedule the task to run daily after the backup job is completed. Click **Start → Settings → Control Panel → Scheduled Tasks**.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

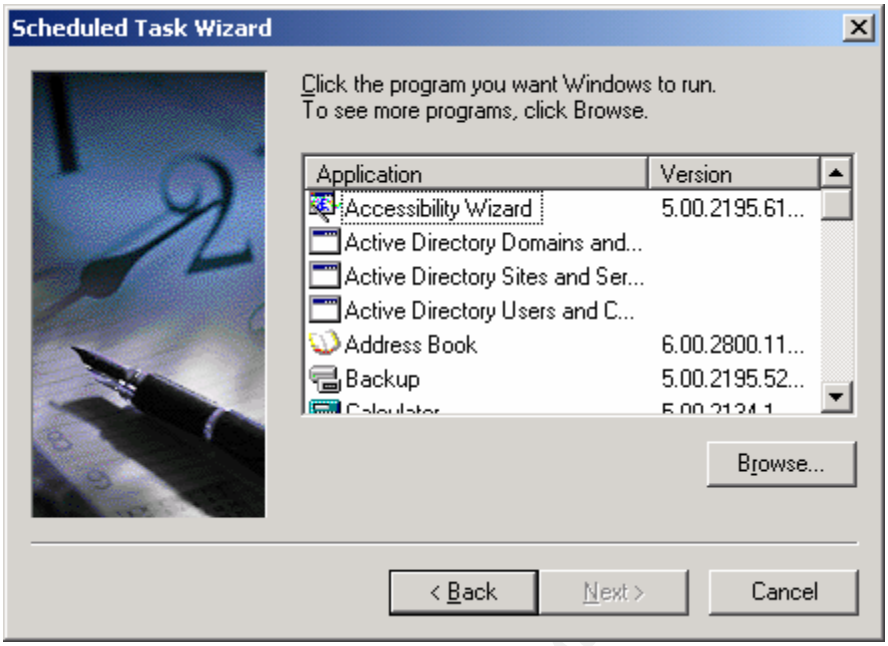


Double-click **Add Scheduled Task**.

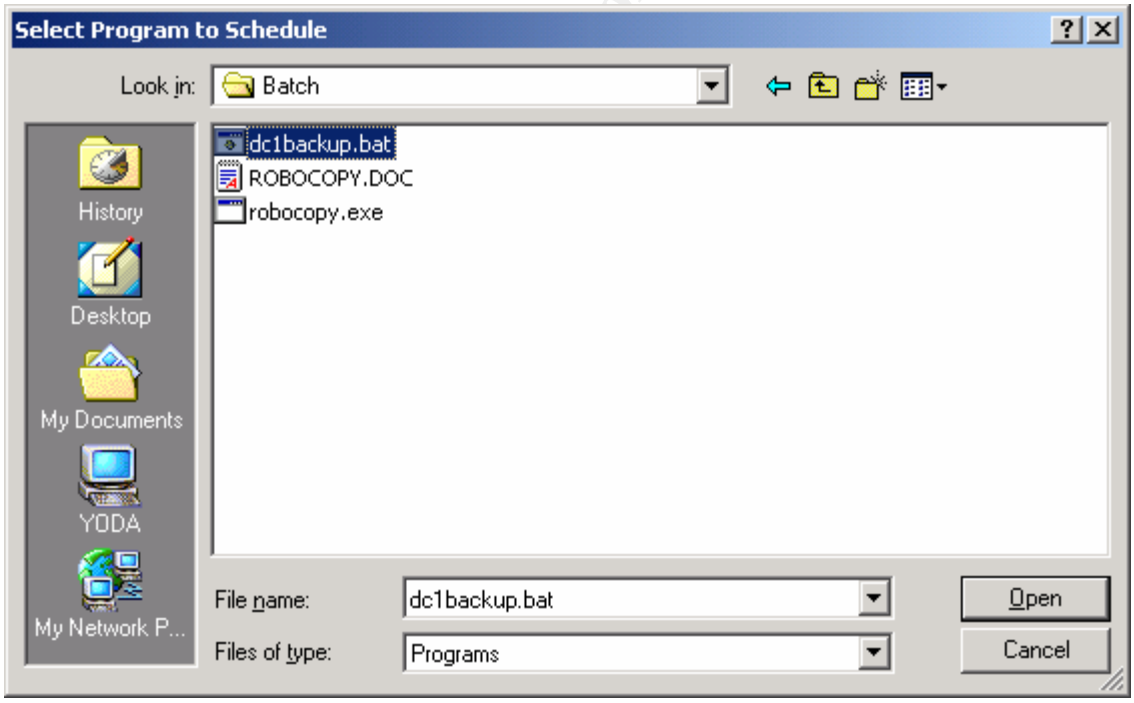


Click **Next >**.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



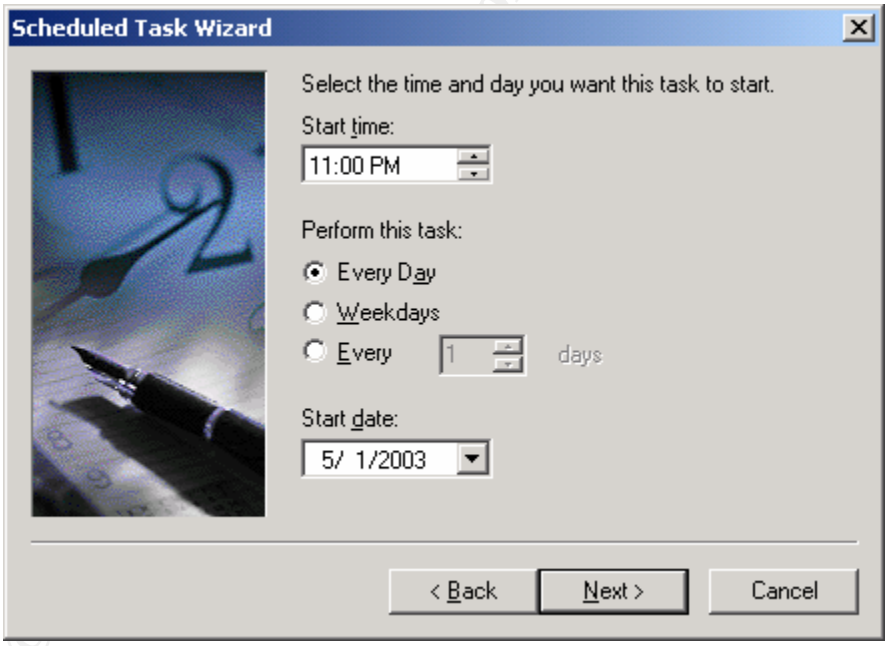
Click **Browse…**.



Browse to the batch file we created and click **Open**.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Enter the name of the task, select **Daily** and click **Next >**.



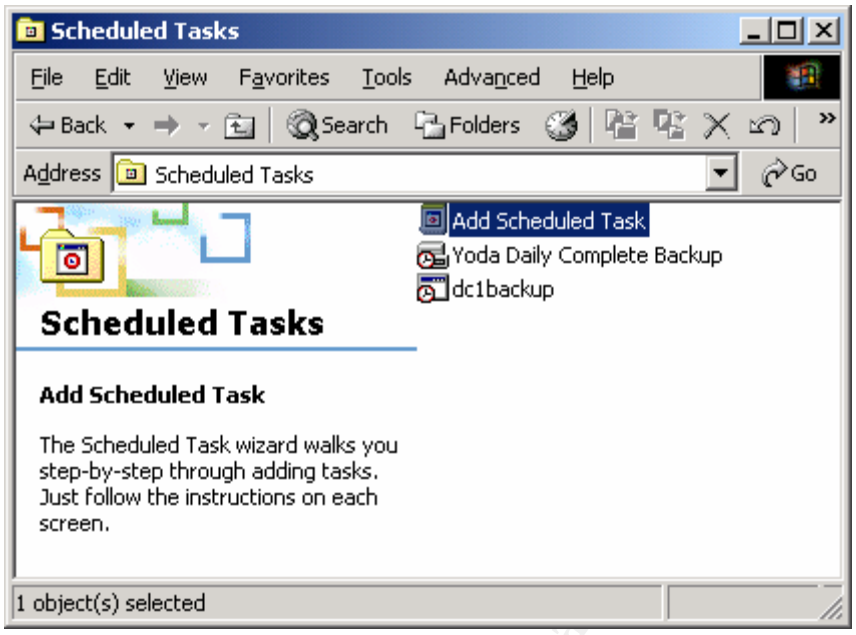
Select the time to start the batch file. Since our backup runs at 8:00 PM, I scheduled the copy to run at 11:00 PM, shortly after the backup is completed. Choose the selection to perform the task every day.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Next, enter the username and password of a domain account to be used for copying of the files. Here, we use an account called *Domain Services* that is used solely for this purpose. This will help when looking through logs as only this account should be used at this time for this function. If you notice that this account is being logged into workstations or other servers, the account may be compromised. Keep in mind that the account you use must be a member of the *Local Administrators* group for both servers. Click **Next >** when finished.

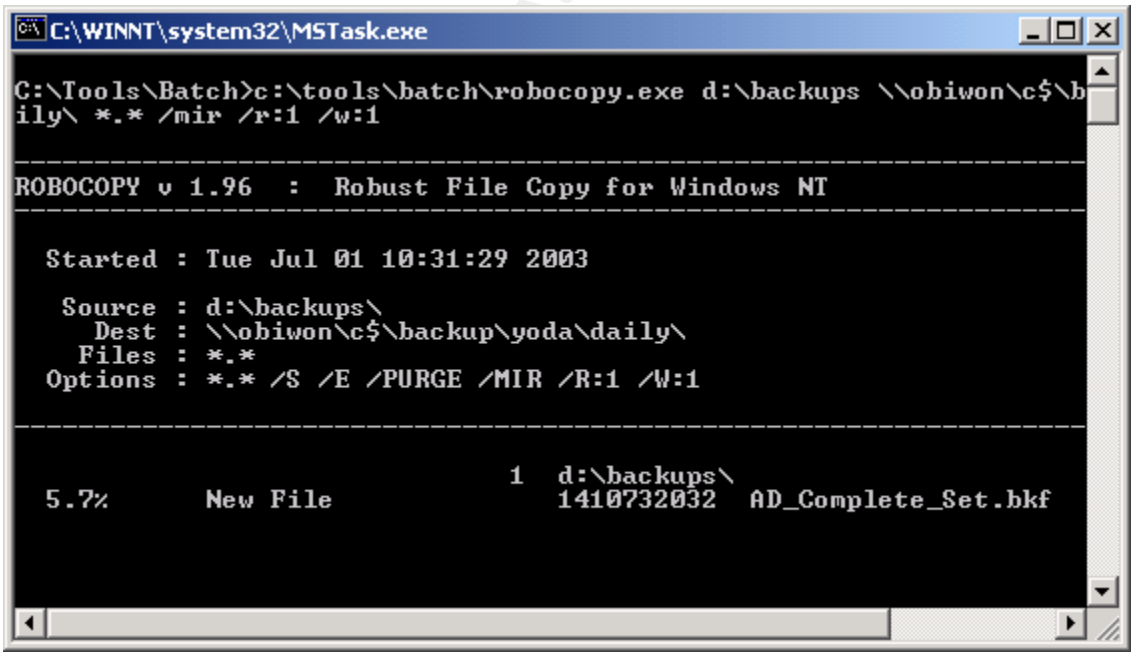
Click **Finish**.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Now you will see the backup which we created earlier, Yoda Daily Complete Backup, and the batch file copy, dc1backup.

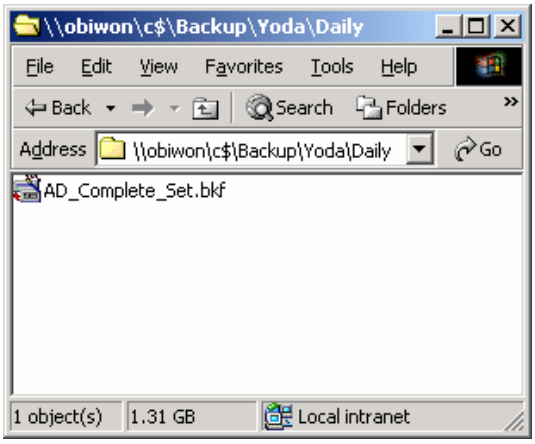
When the *dc1backup* job begins, you will see the following.

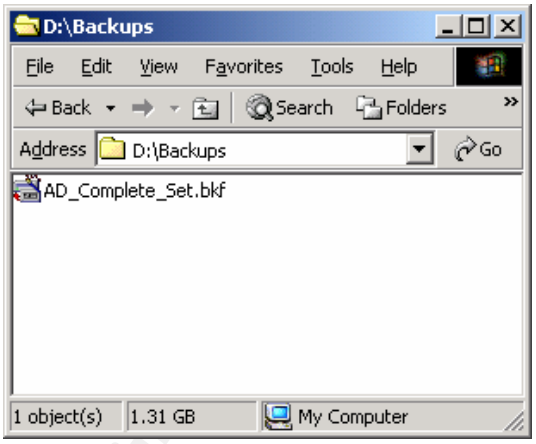


This shows the Robocopy program while it is copying the backup files from the domain controller to the backup server. Afterwards, you may browse to the location you specified for the backup file to be copied to and compare it to the original file on the domain controller. Here, the screen shot on the left is the file that was copied to the backup server, and the screen shot on the right is the file on the domain controller.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Notice that both files are the exact same size, 1.31 GB. The final step would be to transfer the backup from the central backup server to password-protected removable media to store off-site.





Backup Summary

Now, we have created a comprehensive Active Directory backup set in case of a disaster. We should have copies of the Domain Controller backup locally on the Domain Controller itself and the centralized backup server. Additionally, we will have copies of the backup file on removable media generated on the Domain Controller and the centralized backup server.

Fortunately, we are assuming a disaster, so our next step is to restore an entire Active Directory structure from this backup. Please keep in mind that backups must be made for all domain controllers.

Restoring Active Directory

Our first step when planning to restore Active Directory is to rebuild our Domain Controller. If restoring to a hot site, all that should be pre-loaded is Windows 2000 Server, preferably on a machine with the exact same hardware specifications of the server that we are recovering. If the specs are not exactly the same we are still able to restore, but only with a little bit of tweaking of a few .dlls. If you are restoring to a cold site, you will need to install Windows 2000 before restoring. There will be a noticeable time savings if a hot site is used in this situation.

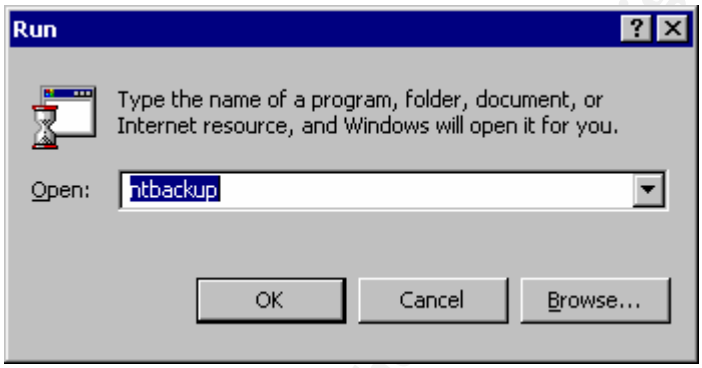
There are a few other special notes with the initial server configuration. First, there is no need to load the proper Service Pack on the server. Since we created a complete backup of our Domain Controller, the Service Pack will be restored during the process. Also, it is not necessary to create the exact same name as the previous server. When the server is restored, the original name will be restored along with its membership to the domain. While Microsoft claims no need to restore drivers, we have found this to be a little

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

misleading. When restoring Active Directory to the same exact hardware, we found the need to reinstall the display driver, so plan to have drivers for all hardware readily available.

Once we have our server in place, our first step is to reboot the server, pressing **F8** at the *Windows Startup Options* screen. Next, select *Directory Services Restore Mode*. The computer will boot into a safe mode so that we may restore Active Directory.

Log on to the server using an account with local administrator privileges. Click **Start → Run...** and enter **NTBACKUP** and click **OK**.

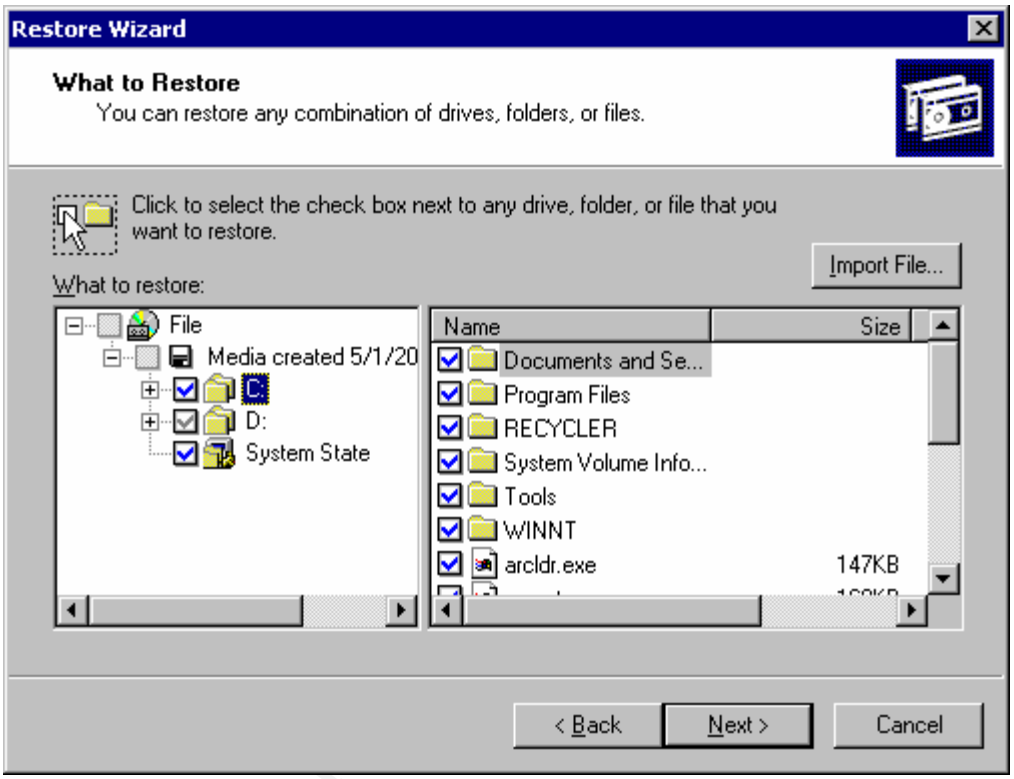


Next, click the **Restore Wizard** button.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

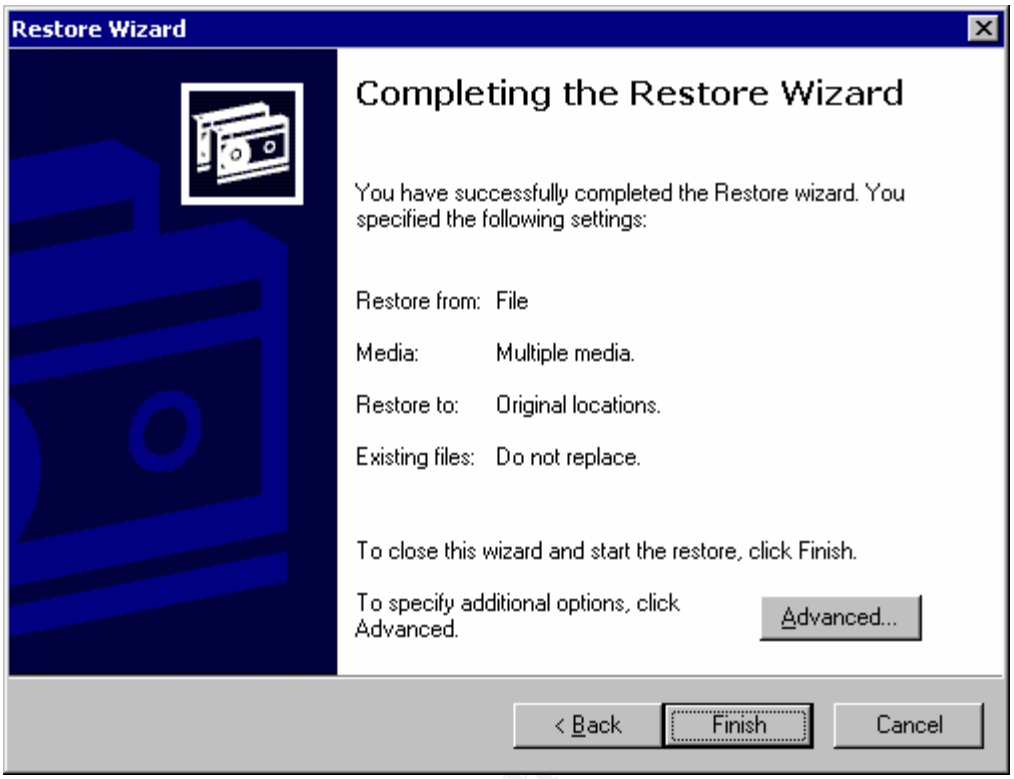
Click **Next** at the initial wizard screen. Click the **Import File…** button and browse to where the backup file is located then click **OK**.

Highlight the selections to restore our server. We will need to restore all system files, along with the system state. In this instance, we are restoring the entire server. Click **Next >** when ready.

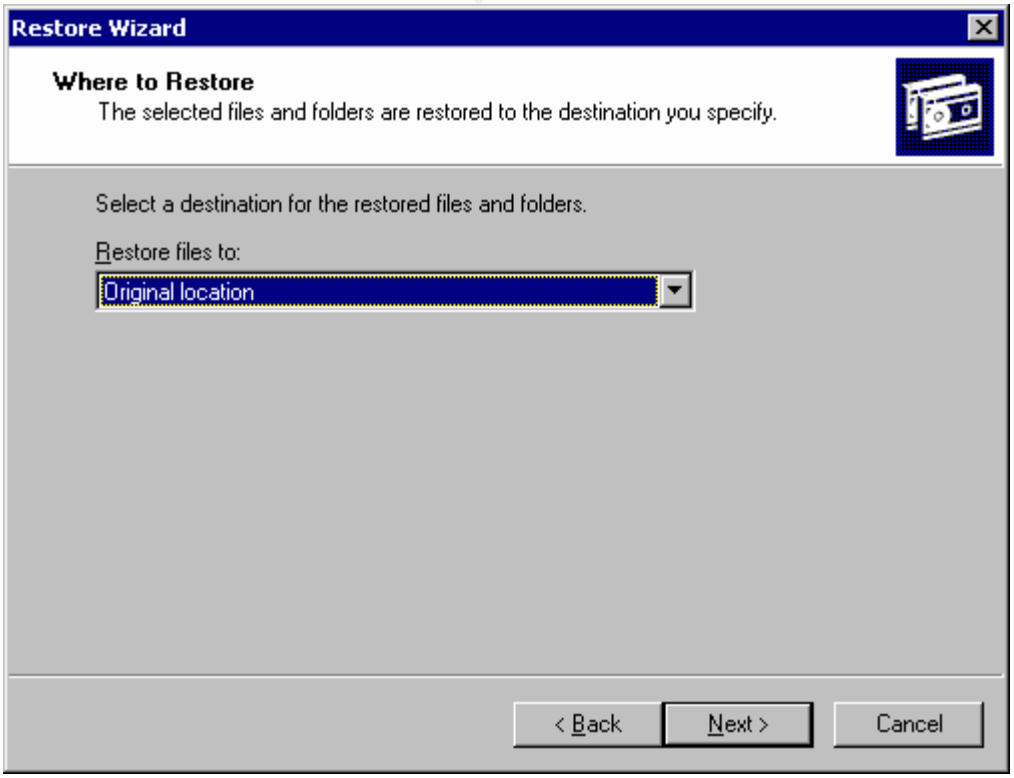


Next, click the **Advanced…** button.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

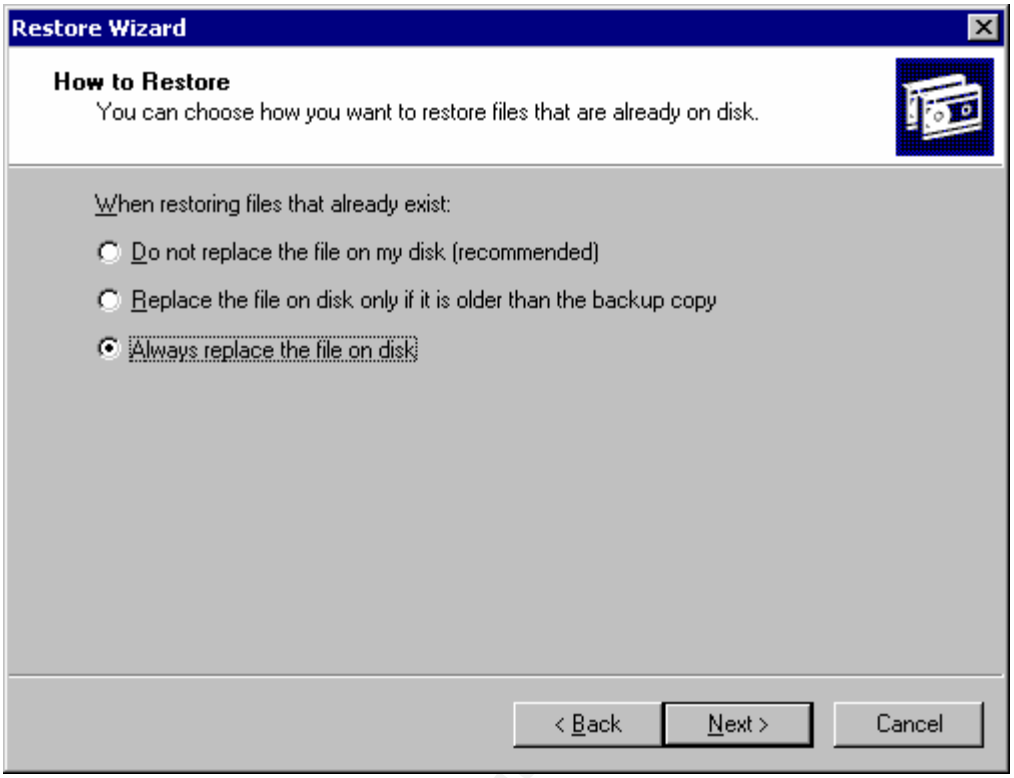


Select to restore the files to their original locations and click **Next >**.

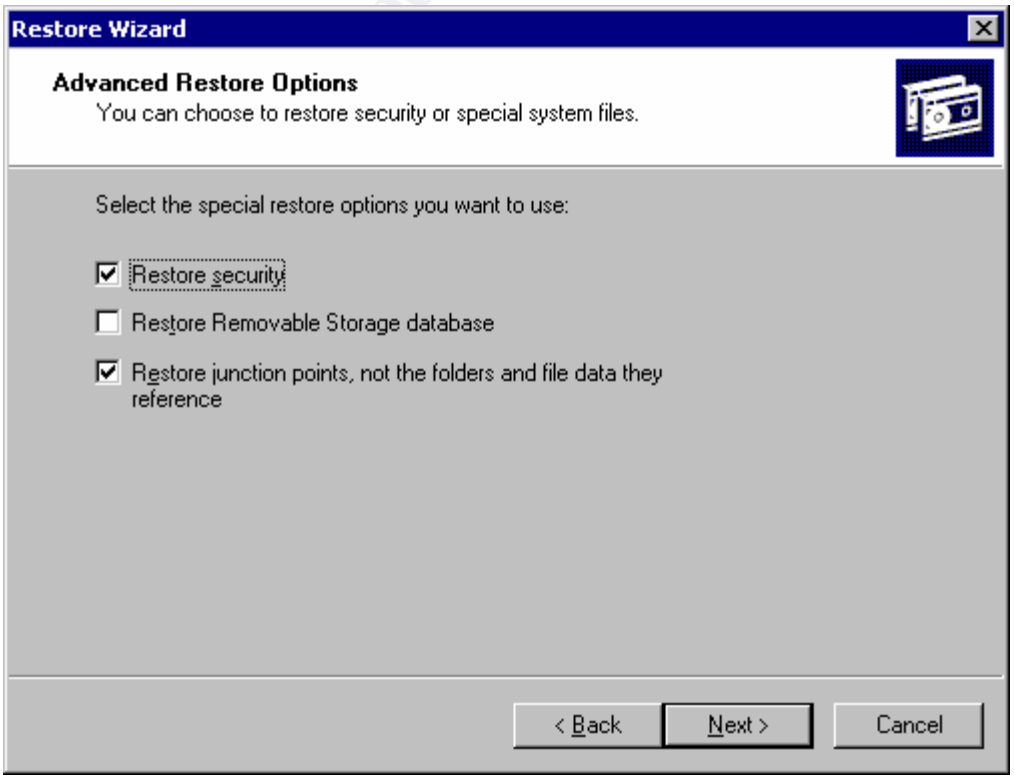


Select the *Always replace the file on disk* option and click **Next >**.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

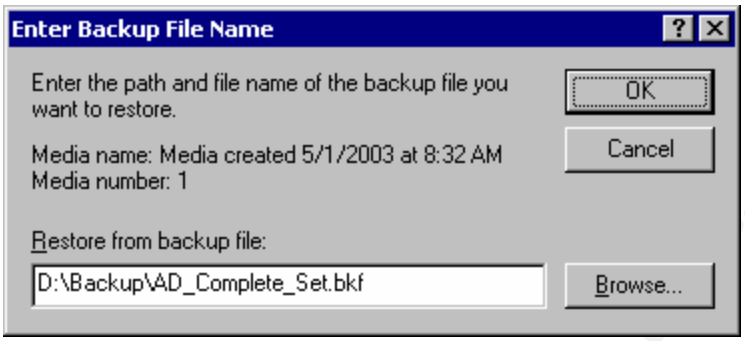


Select the *Restore security* and *Restore Junction Points* check boxes and click **Next >**. Then click **Finish** on the final screen.

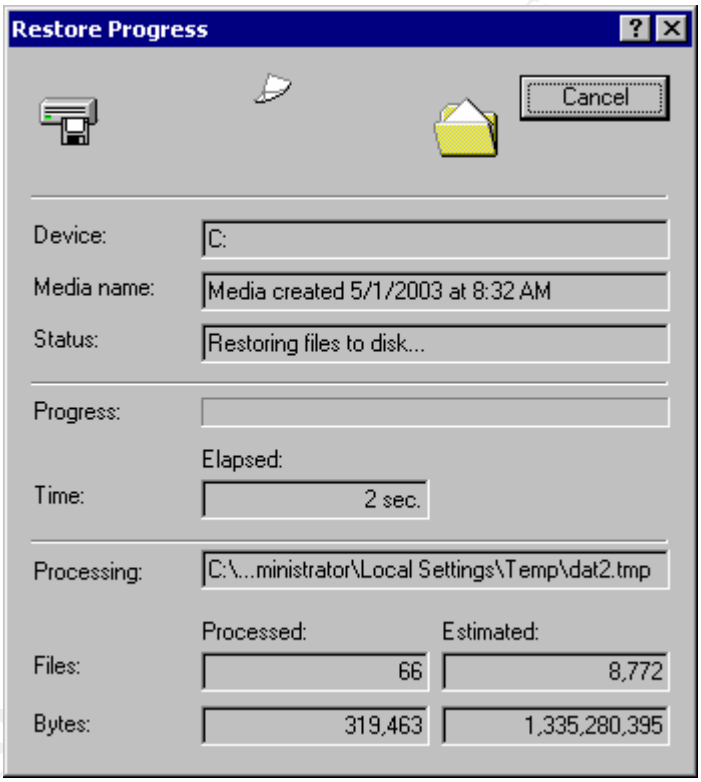


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Click **OK** to the next dialog box that pops up.

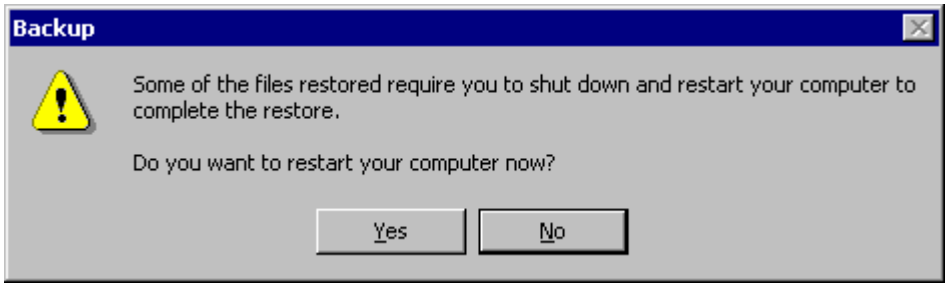


You will see the files being restored.

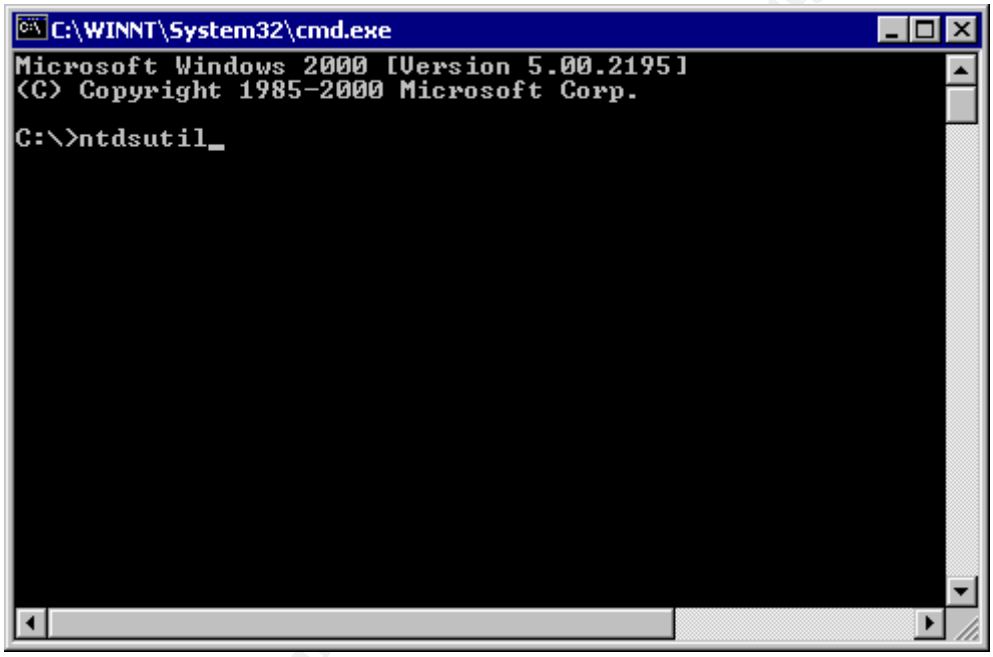


When the restore process is complete, you will be asked to restart the computer. Click **No** at this time.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

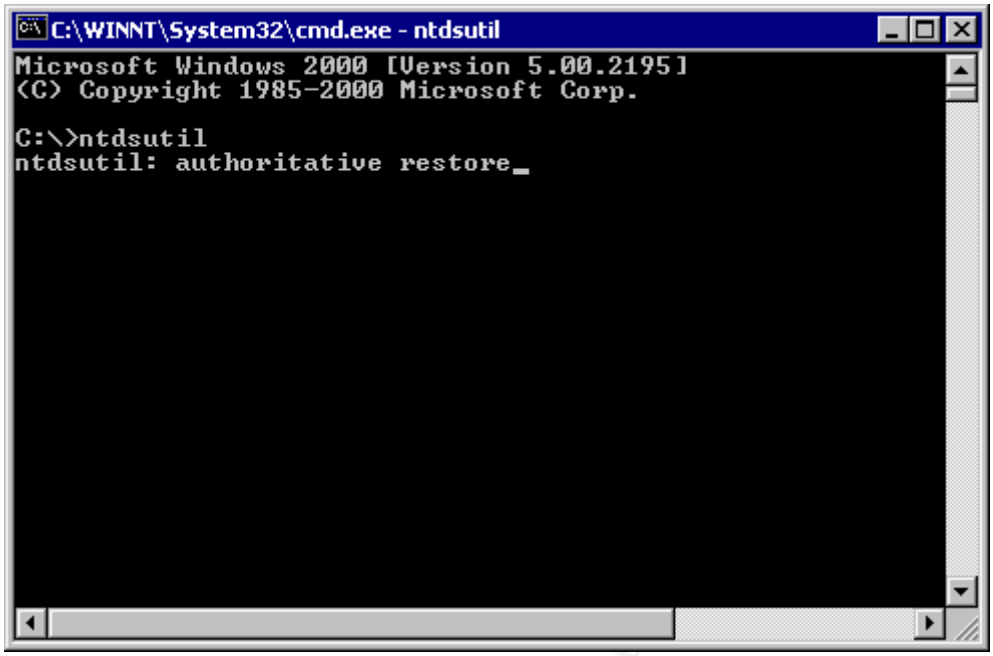


The following steps will need to be entered from a command prompt. First, from the command prompt, type **NTDSUTIL**.

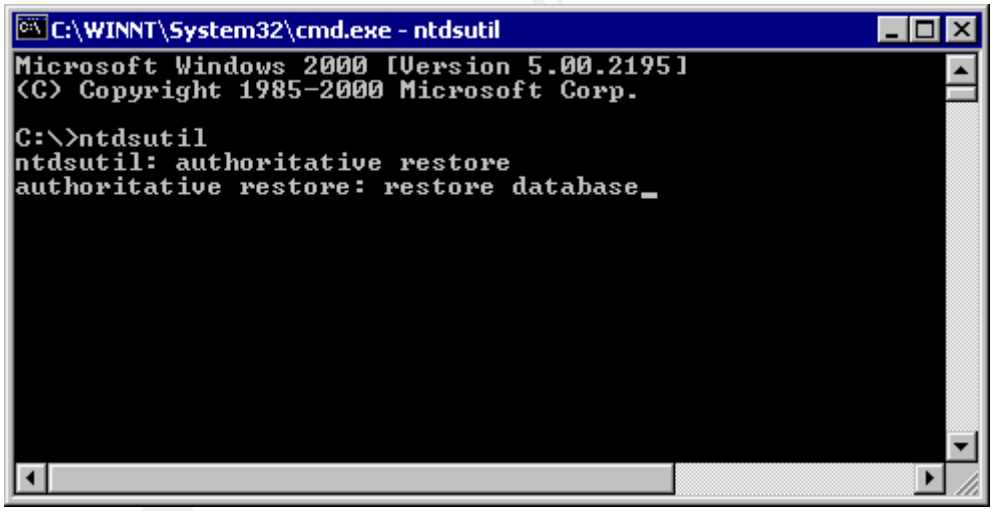


At the next prompt, enter **authoritative restore**.

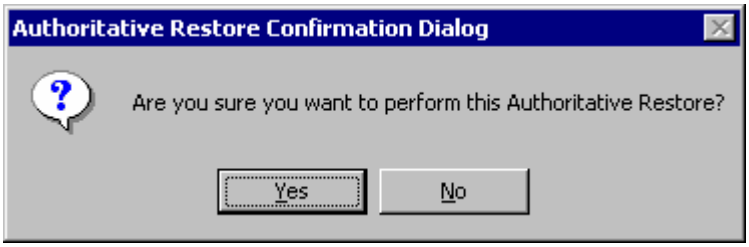
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Now, enter **restore database**.

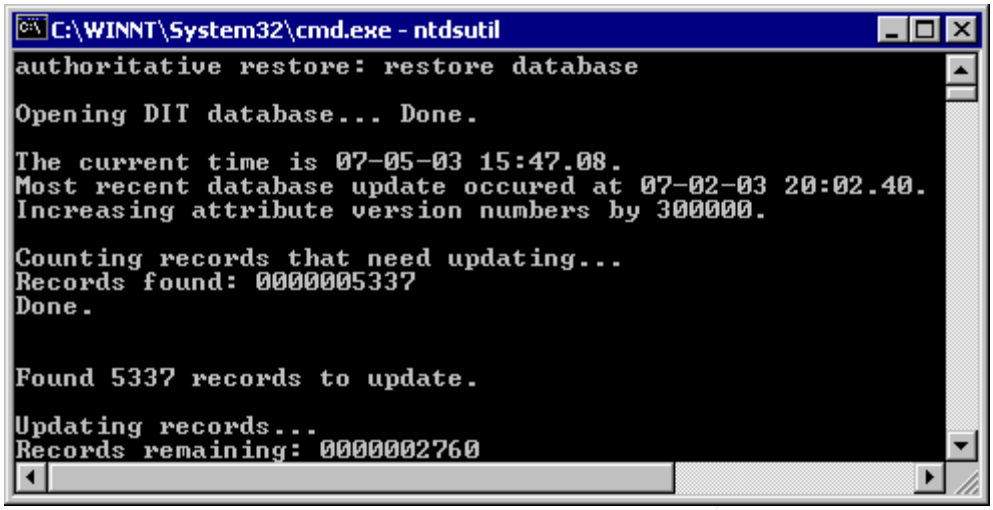


You will be asked to verify your desire to Authoritatively Restore Active Directory. Click **Yes**.



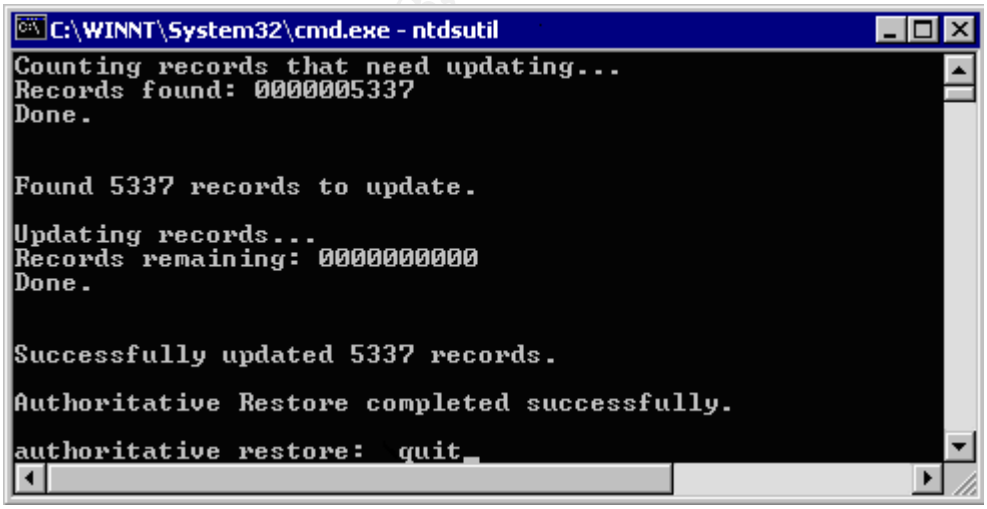
Next, you will see the database restoring itself.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



After Active Directory is done restoring itself, it will increase its Update Sequence Number (USN) by a very large number. In this example, the USN was increased by 300,000. This gives this Active Directory server the highest USN telling other servers to replicate the copy of Active Directory from this server. This process is what makes this type of restore an Authoritative Restore.

When the process completes, enter **quit** at the command prompt until you are completely out of the command prompt interface.



Now restart the computer normally. If you are able to boot into Windows normally, not using any version of *Safe Mode*, then your Active Directory restore is successful. There are a few other things you should look at to verify this though. When you log in, first check the Directory Services Log and check for any errors. Check any other pertinent logs for errors. Next, notice how the server has been restored to its initial Service Pack even though we did not initially update our server when installing.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Conclusion

Active Directory is the heart of any Windows 2000 network. It provides a centralized location for users, groups, and organizational units. It also allows centralized management to deploy application remotely as well as the ability to push security policies to clients. Without Active Directory, users would not be able to access network resources because Active Directory also provides authentication and authorization.

Undoubtedly Active Directory should be included in every Disaster Recovery policy. To backup Active Directory properly in preparing for a complete disaster, a complete backup set of every Domain Controller must be made. A copy of the backup file created should be replicated to a centralized backup server, with both copies then stored off-site. In the event of a complete disaster, close attention should be followed when restoring the Active Directory database.

This document provided a step-by-step analysis of how to backup and restore Active Directory in the event of a disaster. These are just the beginning steps to restore Active Directory. Much more must still be done to complete the restore of an entire network. Some of the steps may vary depending on the setup of the network. Perhaps the best advice of all after creating a plan is to test the plan on a regular basis.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

"Backup of the Active Directory Has 60-Day Useful Life."
http://support.microsoft.com/default.aspx?scid=kb;en-us;216993 (22 April 2003)

"Diagnosing and Troubleshooting Active Directory Problems."
http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/dsbi/dsbi_add_vost.asp

"Disaster Recovery for Microsoft Exchange 2000 Server."
http://download.microsoft.com/download/exchplatinumbeta/Book/1.0/W982KMeXP/EN-US /disasterrecovery.exe (16 September 2002). 118-122.

"HOW TO: Perform an Authoritative Restore to a Domain Controller in Windows 2000."
http://support.microsoft.com/default.aspx?scid=kb;en-us;241594 (27 October 2002)

"Ntdsutil."
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/ntdsutil.asp

"Securing Windows 2000 Active Directory (Part 4) – Restoration."
http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_4__Restoration.html (29 January 2003)

"Windows 2000 Server Disaster Recovery Guidelines."
http://www.microsoft.com/windows2000/docs/recovery.doc (17 February 2000)

Craft, Melissa. Managing Active Directory for Windows 2000 Server. Rockland, MA: Syngress Media, Inc., 2000. 395-441.

Lowe-Norris, Alistair G. Windows 2000 Active Directory. Sebastopol, CA: O'Reilly & Associates, Inc., 2000.

Minasi, Mark. Windows 2000 Server, Fourth Edition. SYBEX, Inc, 2002. 446-586, 1356-1361.

Sandhu, Roopendra Jeet. Disaster Recovery Planning. Cincinnati, OH. Premier Press, 2002. 187-201.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.