

Backing Up Active Directory

Mark E. Donaldson

In Windows NT, all information about user accounts and the enterprise configuration is stored within the Registry. This means that to back up this information, you only have to back up the Registry. However, in Windows 2000, all the security information is stored in the Active Directory. In this article, I'll discuss some of the issues involved in backing up and restoring the Active Directory.

Background

Before I delve deeply into the issues involved in backing up and restoring the Active Directory, I should tell you something about the limitations of this process. For starters, the Active Directory can only be backed up as a part of a normal backup—you can't perform an incremental or a differential backup and expect to back up the Active Directory.

You also can't make a backup of just the Active Directory. Windows 2000 backs up the Active Directory as a part of the system state data. The system state data includes interdependent items such as the Registry, system startup files, class registration database, certificate services database, file replication service, cluster service, domain name service, and Active Directory. Unfortunately, none of these items can be backed up separately—they must all be backed up as a part of the system state.

Because of the way that Windows 2000 requires you to back up system state information, it should come as no surprise that doing so requires you to use a backup program specifically designed for Windows 2000. A Windows NT backup tool will work fine for backing up data files, but it won't contain the necessary code for backing up the system state data. If you don't have such a program, you can use the backup program that's included with Windows 2000. Note, however, that no one server contains the entire Active Directory. If you plan to use the Windows 2000 backup program, you must back up the system state on each server in order to back up the entire Active Directory. Some third-party backup programs will allow you to back up remote system states; however, limitations in the Windows 2000 backup program prevent it from doing so.

Backing up the Active Directory

Here's a list of the files that compose the Active Directory:

- ntds.dit--The database
- edb.chk--Checkpoint file
- edb*.log--Transaction log files
- res1.log and res2.log--Reserved transaction log files (used in case the server runs out of hard disk space)

As I mentioned earlier, the Active Directory can only be backed up along with the system state data. To back up the system state data, follow these steps:

1. Select Start|Run and enter the ntbackup command. When you do, you'll see the NTBACKUP tool.
2. Select Tools|Backup Wizard. When the Backup Wizard starts, click Next, select Only Backup System State Data, and click Next again.
3. Designate the location that you want the system state backed up to. Click Next followed by Finish.

If you're backing up the system state to a file, I recommend placing the file on a partition that's running the Windows 2000 version of NTFS. Doing so will help ensure that no information is lost during the backup process.

Backing Up Active Directory

Mark E. Donaldson

Restoring the Active Directory

You can use two basic methods for restoring the Active Directory. The first method involves reinstalling Windows 2000. Once Windows 2000 has been reinstalled as a domain controller, you can allow the other domain controllers to populate the Active Directory through the normal replication process. Doing so will keep the Active Directory in its current state.

Another method involves restoring the Active Directory from the backup media. Doing so will restore the Active Directory to the state that it was in at the time of the last backup.

Rebuilding Through Replication

As I mentioned, if your server totally crashes, you can reformat it and reinstall Windows. You can then let the other Windows 2000 domain controllers populate the database on the newly reinstalled server.

To do so, select Start|Programs|Administrative Tools|Active Directory Sites And Services on an existing domain controller. Then, delete any references to the damaged domain controller. You can now safely reinstall Windows 2000 onto the damaged server. During the course of the installation, set the server to be a domain controller in the domain that it once belonged to. Once Setup completes, the Active Directory will be replicated from an existing domain controller to the newly reinstalled server.

Restoring from Backup

Restoring from the backup media brings the Active Directory database to the state it was in at the time of the last backup. You have two options when restoring the system state data from a backup tape: an authoritative restore or a nonauthoritative restore. Before I get into the differences, I need to mention an issue associated with restoring system state data.

Suppose for a moment that your server's information was completely destroyed due to a hardware failure. Obviously, before you could restore anything, you'd have to fix the problem and reload Windows. When doing so, keep in mind that for the restore to work correctly, you'll have to reinstall Windows 2000 onto the same partition it was previously loaded on. Once you've reloaded Windows 2000, you must recreate the partitions that existed before at their previous size or larger.

Authoritative restore vs Non-authoritative Restore

By default, Windows 2000 uses a nonauthoritative restore: Active Directory is restored from the backup media. Later, however, the other domain controllers may overwrite portions of the restored data with newer data. For example, suppose that today is Friday and you just restored an Active Directory from Wednesday. Any changes in the Active Directory that have occurred since Wednesday will be automatically replicated to the server you've just restored, even if it means overwriting portions of the Active Directory.

An authoritative restore, on the other hand, takes precedence over Active Directory information that's stored on all other domain controllers. This is true regardless of the age of the information that you've just restored. An authoritative restore is useful when you need to return the entire Active Directory to a previously known state. For example, suppose the Active Directory on a server has become badly damaged. Now suppose the damaged Active Directory has been replicated to all domain controllers, thus making their Active Directories unusable. An authoritative restore could be used to restore a known good Active Directory database and replicate it to all of the domain controllers, thus repairing their databases at the same time.

Backing Up Active Directory

Mark E. Donaldson

Non-authoritative Restore

To perform a nonauthoritative restore, the directory services database must be offline (the database doesn't have to be offline during the backup). To restore the Active Directory, you must place the server into Directory Services Restore Mode. To do so, reboot the server. When you see the screen that asks you to select your operating system, press F8. You'll see a menu with various diagnostic and recovery options. Select the Directory Services Restore Mode command from this menu and press Enter.

Windows will now appear to boot normally. However, you must log in using the local administrator's account and password. Keep in mind that because the Active Directory has been taken offline, it's impossible to log in to the domain. Therefore, the only accounts that you can use to log in are those stored within the security accounts manager database (sometimes called the SAM).

Once logged in, you may begin restoring the Active Directory:

1. Select Start|Run and enter "ntbackup" at the prompt. Windows 2000 will load the backup program.
2. Select Tools|Restore Wizard. Click Next to clear the welcome message. The backup program will display the backup sets that are available for restore.
3. Select the backup set you want to use and navigate through the backup set to find the system state option. Select the System State check box and click Next followed by Finish.

It's important to point out that Windows 2000 won't let you restore system state data that's older than the default tombstone lifetime. The default tombstone lifetime is the amount of time that a deleted object is maintained within the Active Directory before the garbage collection process clears it out. By default, this period is set to 60 days. So, unless you do some tweaking, you can't restore Active Directory information that's older than 60 days.

Upon completion of the restore operation, the file replication service is reset so that replication may begin. You may then reboot your server in the normal manner. Upon rebooting, Windows 2000 will perform a consistency check against the Active Directory and reindex the files that make up the Active Directory database. Windows will also begin the replication process with its replication partners and restore the certificate services database if appropriate.

Authoritative Restore

To perform an authoritative restore, you must first perform a nonauthoritative restore. Then, you can use the NTDSUTIL tool to make the restored Active Directory authoritative. An authoritative restore can be used to replace an entire Active Directory or just a portion of it.

To perform an authoritative restore, use the process I discussed earlier to restore the system state. When the restore process completes, don't reconnect to the network--instead, reboot the computer. When you see the screen that asks which operating system you want to use, press F8. You'll see the same diagnostic menu you saw earlier; select the Directory Services Restore Mode command and press Enter.

Windows will now load. Log in to Windows using the local administrator's account as you did earlier. Select Start|Run and execute the ntdsutil command. To restore the entire database, enter the following commands:

Backing Up Active Directory

Mark E. Donaldson

```
authoritative restore  
restore database
```

If you want to restore only a portion of the database, you can use the following commands (of course, substitute your own sub tree):

```
authoritative restore  
restore subtree ou=Brien,dc=files,dc=COM
```

At this point, type "quit" and restart the server in the normal manner.

Authoritatively Restoring Group Policies

Keep in mind that the directory service database may have group policies associated with it. These group policies are stored in the SYSVOL directory. To make sure that the group policies in the SYSVOL folder are correct, restore the system state data to its original location and to an alternate location.

After you've used the NTDSUTIL tool to make the Active Directory authoritative and rebooted the computer, Windows will publish the contents of the SYSVOL folder. Once the SYSVOL folder has been published, overwrite the SYSVOL folder with the one stored in the alternate location. If you're only authoritatively restoring a portion of the Active Directory, wait until the SYSVOL folder has been published and then overwrite only the policy folders that correspond to the restored policy objects. You can determine which folders and objects are associated by looking at the GUID. //