NTDSutil commands 2

NTDSutil is a wonderful Windows utility for configuring the heart of Active Directory. In fact, typing the powerful NTDSutil verbs reminds me of a Unix command line.

With NTDSutil you get instant access to the Active Directory database. Unlike GUIs, which drive me mad with their 27 OK buttons, NTDSutil just does what I say - instantly. However, because these NTDSutil commands act without the usual Windows operating system checks, I exhort you to practice my examples now, don't wait until you need them in a real disaster recovery. As a bonus of following my tutorials, you will discover settings that you did not know existed, for example, choose a new password for DSRM (Directory Service Restore Mode).

Preparation for NTDSutil

Begin by logging on at a Windows Server. I suggest that you create a new folder to hold any logs that NTDSutil creates, for example D:\ ntdsutil. Run a CMD prompt change directory to D: \ntdsutil and at the prompt type, ntdsutil. Unsurprisingly, the actual executable is called ntdsutil.exe and is found in the %systemroot%\system32 folder. With this knowledge, you could copy that ndtsutil.exe file onto another operating system if necessary.

Key NTDSutil command

When you are experimenting with NTDSutil, if you get stuck remember these four little words, they will make the difference between success and frustration:

Connect to Server BigServer (Substitute your server for BigServer)
Don't shorten the command to: Connect BigServer (Remember the words 'to' and 'server').

If ever you are stuck in NTDSutil, simply type **help**.

NTDSutil tasks

- **Authoritative Restore** - Major project, needs careful planning.
- **Configurable Settings** - Not very interesting.
- **Domain Management** - Specialist area. Create Naming Contexts and add replicas to the Application Directory Partition of DNS.
- **Files** - Available only if you boot the server into Directory Restore Mode. Checks the integrity of NTDS.DIT and moves associated databases.
- **Roles** = FSMO Maintenance. Which Domain Controller has which Single Operations Master? Seize roles such as PDC Emulator. Good news, for once you do get a message detailing the transfer you are about to make.
- **Reset DSRM password**. If you don't know the server's Directory Service account password, then here is your change to reset to a password that you will remember.
- **Security Account Management**. Check for duplicate SIDs

Example 1: Security Account Management (Maintenance)

Let us start gently and check for duplicate SIDs. This experiment is more for gaining experience of the NTDSutil interface than the probability of finding any duplicate SIDs. This is what I typed at the command prompt, my commands are in bold:

```
E:\ntdsutil>ntdsutil
ntdsutil: security account management
Security Account Maintenance: connect to server BigServer
Security Account Maintenance: check duplicate sid
...
Duplicate SID check completed successfully. Check dupsid.log for any duplicates
Security Account Maintenance:
```

1. In the above session I typed the full command **security accounts management**. However you can shorten commands thus: 'sec acc man'

   Incidentally, I am inventing these shorthand commands in the sense that NTDSutil also understands: sec ac ma or even 'secu a m'. NTDSutil's brain works by analysing your letters and if there is only one possible interpretation then it fills in the gaps and returns the service that you asked for. For example plain, 'se' will not work because there is another command which begins with se, Semantic....

2. When the command prompt shows, Security Accounts Maintenance:
   Here is where you must type: 'connect to server BigServer'. Be aware that even though I am sitting at BigServer's console, I must remember this command : connect to server xyz.

3. When I type the instruction, 'Check Duplicate SID', don't ask me why, but you cannot shorten the command to 'chk dup sd'. Please just accept you need the full words here.

4. As ever, read the screen and take note of dupsid.log. However, you have to quit NTDSutil, or use Explorer before you can attempt to read dupsid.log. My point is that you cannot issue a command : 'notepad dupsid.log' from within NTDSutil.

Example 2: Reset password for DSRM (Directory Services Restore Mode)

Here is where I challenge you to perform a real task. Once upon a time, when your Windows server 2003 was first installed, setup asked the installer for a separate directory service restore mode password. 90% of administrators ignored the box or forgot the password. 50% of Administrator's don't realize that this Directory Services Restore Mode password is different from the normal Administrator password. The two can get out of synch because they are stored in separate databases.

Now is your chance to reset the password that will be required if ever you need to restart the server in Active Directory Restore Mode. In many ways, this is such an insignificant job, in other ways it saves frustration of being thwarted by not having the administrative password for this context.

```
E:\ntdsutil>ntdsutil
ntdsutil: set dsrm password
Reset DSRM Administrator Password: reset password on server BigServer
Please type password for DS Restore Mode Administrator Account: ********
Please confirm new password: ********
Password has been set successfully.

Reset DSRM Administrator Password: quit
ntdsutil: quit

E:\ntdsutil>
```

1. The key command type: 'reset password on BigServer'
   If NTDSutil replies with: 'Please type password for DS Restore Mode', then you know you are in the correct place.

2. To escape from NTDSutil you need just type quit, possibly 2 or three times to get back to the command prompt.

Summary of NTDSutil

NTDSutil is a powerful command line tool. Take every opportunity to practice its Unix-like commands. If you practice with NTDSutil then you will be prepared for that day when you need to employ NTDSutil for disaster recovery tasks such as an Authoritative Restore.

How to Start Your Computer in Directory Services Restore Mode

Windows Server 2003 Directory Service opens its files in exclusive mode. This means that the files cannot be managed while the server is operating as a domain controller.

To start the server in Directory Services Restore mode, follow these steps:

1. Restart the computer.
2. After the BIOS information is displayed, **press F8**.
3. Use the DOWN ARROW to select **Directory Services Restore Mode (Windows Server 2003 domain controllers only)**, and then press ENTER.
4. Use the UP and DOWN ARROWS to select the Windows Server 2003 operating system, and then press ENTER.
5. Log on with your administrative account and password.

How to Install Support Tools and Start Ntdsutil

To install Windows Support Tools, follow these steps:

1. Insert the Windows Server 2003 installation CD in the CD-ROM or DVD-ROM drive.
2. Click **Start**, click **Run**, type ***drive_letter:*\Support\Tools\suptools.msi**, and then press ENTER.

To start Ntdsutil, click **Start**, click **Run**, type **ntdsutil** in the **Open** box, and then press ENTER.

NOTE: To access the list of available commands, type **?**, and then press ENTER.

How to Move the Database

You can move the Ntds.dit data file to a new folder. If you do so, the registry is updated so that Directory Service uses the new location when you restart the server.

To move the data file to another folder, follow these steps:

1. Click **Start**, click **Run**, type **ntdsutil** in the **Open** box, and then press ENTER.
2. At the Ntdsutil command prompt, type **files**, and then press ENTER.
3. At the file maintenance command prompt, type **move DB to *new location*** (where new location is an existing folder that you have created for this purpose), and then press ENTER.
4. To quit Ntdsutil, type **quit**, and then press ENTER.
5. Restart the computer.

How to Move Log Files

Use the move logs to command to move the directory service log files to another folder. For the new settings to take effect, restart the computer after you move the log files.

To move the log files, follow these steps:

1. Click **Start**, click **Run**, type **ntdsutil** in the **Open** box, and then press ENTER.
2. At the Ntdsutil command prompt, type **files**, and then press ENTER.
3. At the file maintenance command prompt, type **move logs to *new location*** (where new location is an existing folder that you have created for this purpose), and then press ENTER.
4. Type **quit**, and then press ENTER.
5. Restart the computer.

How to Recover the Database

To recover the database, follow these steps:

1. Click **Start**, click **Run**, type **ntdsutil** in the **Open** box, and then press ENTER.
2. At the Ntdsutil command prompt, type **files**, and then press ENTER.
3. At the file maintenance command prompt, type **recover**, and then press ENTER.
4. Type **quit**, and then press ENTER.
5. Restart the computer.

NOTE: You can also use Esentutl.exe to perform database recovery when the procedure described earlier in this article fails (for example, the procedure may fail when the database is inconsistent). To use Esentutl.exe to perform database recovery, follow these steps:

1. Click **Start**, click **Run**, type **cmd** in the **Open** box, and then press ENTER.
2. Type **esentutl /r *path*\ntds.dit**, and then press ENTER. path refers to the current location of the Ntds.dit file.
3. Delete the database log files (.log) from the WINDOWS\Ntds folder.
4. Restart the computer.

For additional information about the esentutl.exe utility, at the command prompt, type **esentutl /?**, and then press ENTER.

NOTE: This procedure involves transaction logs to recover data. Transaction logs are used to make sure that committed transactions are not lost if your computer fails or if it experiences unexpected power loss. Transaction data is written first to a log file, and then it is written to the data file. After you restart the computer after it fails, you can rerun the log to reproduce the transactions that were committed but that were not recorded to the data file.