Ten Useful NT Resource Kit Utilities

The Windows NT Resource Kit is regarded by many as almost part of the OS, and as an NT administrator it's well worth getting your hands ona copy. We round up the most useful 10 utilities to be found in the Kit and explain how best to use them.

By Simon Pride

If I were asked for the most useful piece of advice I could give to beginning or intermediate Windows NT system administrators, it would be to view the Resource Kit utilities as mandatory rather than optional. I am sometimes known to describe the NT Resource Kit books as "the real NT manual" and its associated utilities as "the bits of NT that got left out".

Microsoft is notorious for playing its technical cards very close to its chest when it comes to documenting how bits of NT (or Windows 95 or 98, for that matter) actually work, but the Resource Kit books provide a reasonable overview of the nuts and bolts of NT.

Similarly, the Resource Kit utilities provide the missing commands and tools that system administrators coming from a Unix, VMS or even NetWare background are used to having. (Although, as an aside, the NetWare situation is in some ways similar in that many Novell administration functions are eased or even made possible by the excellent JRButils from JRB Software, which can be found on the Web at **nz.com/webnz/JRBSoftware/**.)

You can get the Resource Kit in two ways: either by buying the Microsoft Press book *Windows NT Resource Kit*, which includes a CD of the Resource Kit utilities, or by subscribing to Microsoft's TechNet programme.

TechNet consists mainly of a set of CDs containing the Microsoft Knowledgebase, the full text of many important manuals (such as those for the whole of BackOffice) and of the various Resource Kits, plus the latest version of the Resource Kit utilities. I'd also go as far as to say that, for the serious technical support professional in a Microsoft environment, TechNet is not optional either.

You can also get the information in the Resource Kit books from Microsoft's MSDN section of its vast and constantly changing Web site. I shall not give a URL for this, since the site is so dynamic it is likely to be out of date before this article reaches you; instead, go to **www.microsoft.com,** look for Developer information and follow links to the MSDN library. Note that in order to access the information your Web browser will need to support Java, as the interface to the library is a Java applet.

The Resource Kit utilities are of two types: the command-line utilities which carry out the same functions as

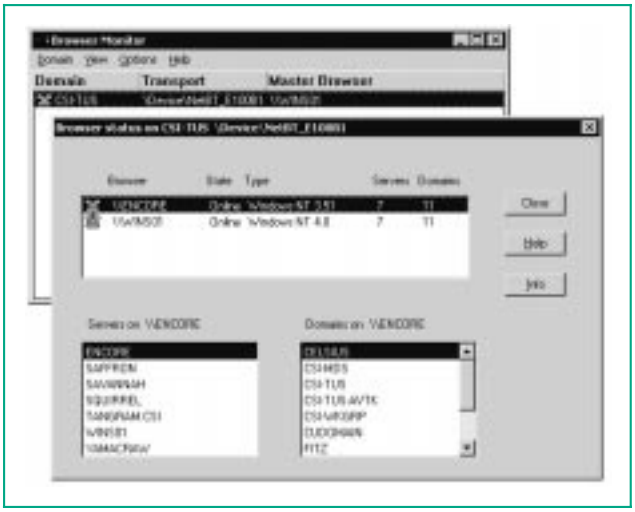

Figure 1 - Browser Monitor showing Domain Master Browsers.

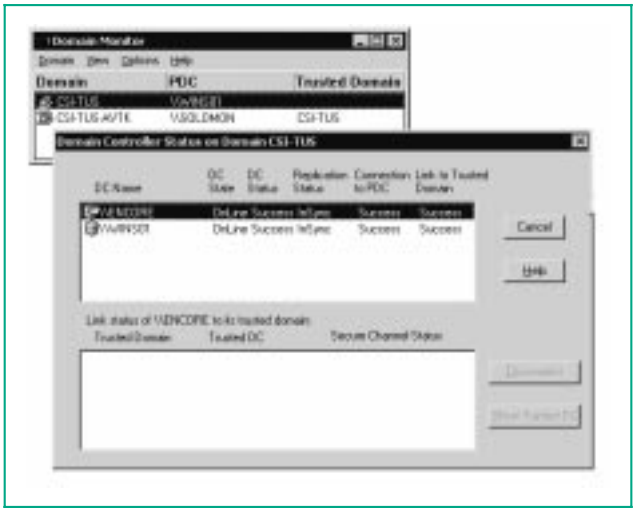

Figure 2 - Domain Monitor showing Domain Controllers for a domain.

"For each logical network in use on the LAN (LANAs in Microsoft network terminology) Browser Monitor reports the current Master Browser for each transport in use on the network segment."

the standard NT GUI equivalents, but have the obvious benefit that they can be called from scripts and passed arguments from other scripts; and the extra GUI tools which tap into areas of functionality not exposed by the standard NT user interface. Without further ado let's dive in and look at some of the ones I use most often.

GUI Tools

NT provides facilities for automatically running programs or scripts at certain times of day via the Schedule service (equivalent to Unix's cron daemon) and the AT command, which provides a command-line interface to the service, using which the system administrator can schedule jobs for later execution.

However, many system administrators have found AT's syntax difficult, and therefore Microsoft has provided a graphical interface to the schedule service in WinAT.

WinAT

If you installed the Resource Kit utilities with the CD's SETUP program you will find WinAT under Start\Programs[common group]\Resource Kit 4.0\Configuration\Command Scheduler. Running it for the first time opens a blank scheduler document representing a single computer (like most NT utilities, WinAT can work on a remote NT computer as easily as on the local one).

To create a new scheduled job, choose Edit/Add and type the path and command line to the script you want to execute. You may be tempted to put the name of a binary executable on this command line, but if you do you will usually find that it doesn't work.

I have not yet found documentation for this, but it is an established part of NT folklore that the only way of running a program successfully using the Schedule service is to wrap it in a script. Furthermore, you must invoke the script with an explicit launch of a command shell, passing it the name of the script as a command-line argument:

```
CMD /C "C:\MyPath\MyCmd.cmd"
```

Another reason for programs scheduled with WinAT or even the AT command to fail is if Microsoft Internet Explorer 4 or 5 has been installed on the computer in question. IE replaces the native NT ATSVC.EXE with its own schedule service MSTASK.EXE, which is incompatible with AT and WinAT. Microsoft KnowledgeBase article Q196731 describes how to rectify the situation (this can be found on the Web at **support.microsoft.com/support/kb/articles/q19 6/7/31.asp**).

For another interface to the AT command and schedule service see the section on SOON below.

Browser Monitor/Domain Monitor

These two GUI applications perform similar functions in a Microsoft networking environment. For each logical network in use on the LAN (LANAs in Microsoft network terminology) Browser Monitor reports the current Master Browser for each transport in use on the network segment (see Figure 1). This tool is very useful for diagnosing resource location problems due to browser wars (constant browser elections).

Domain Monitor lists the Primary Domain Controller for visible domains and the domains with which it has established trust relationships - see Figure 2.

Command-Line Tools

ADDUSERS, NTRIGHTS, XCACLS, GLOBAL and LOCAL are command-line equivalents to User Manager (for Domains) and the Permissions tab of the NTFS properties dialog.

ADDUSERS

ADDUSERS takes a specially formatted text file as input and creates user accounts, complete with home directories and the connections to logon scripts and profiles. [Note that the for-

```
REM Script to demonstrate use of command line security tools
REM Dump all users from Domain Users
REM Assumes that Resource Kit security utilities are on the path
IF EXIST DU.TXT DEL DU.TXT
GLOBAL "Domain Users" MYDOMAIN > DU.TXT
REM Now open the file and pass each entry as an argument to NTRIGHTS
REM Revoke the right to log on at the Domain Controller
FOR /F "tokens=1" %%A IN (DU.TXT) DO NTRIGHTS -r SeInteractiveLogonRight -
u %%A
REM more restrictions of undesirable rights here
REM set some file permissions, starting with revocation of the ability to
write to the Windows System32 directory
FOR /F "tokens=1" %%A IN (DU.TXT) DO XCACLS %SYSTEMROOT%\SYSTEM32 /E /R
%%A:W;W
...etc....
```

Figure 3 - A script to reset the security properties of users to a known base level.

Resource Kit

mat of the source file given in the Resource Kit documentation is incorrect. The correct format is shown in *How To Manage NT User Accounts*, PCNA 108, File T1711, Figure 4.]

NTRIGHTS

NTRIGHTS grants and revokes NT user rights from the command prompt in the same way that XCACLS can grant permissions. The NTRIGHTS syntax is:

```
NTRIGHTS [+|-]r <right to add> -u
<user or group>
```

The <right to add> must be specified as NT's internal name for the right and is case-sensitive. A list of the internal names for rights is given in the Help file for the Resource Kit tools.

XCACLS

This utility allows the administrator to set permissions for users and groups by changing the ACL entries for files and directories (folders). XCACLS allows the setting of individual permissions, whereas CACLS only worked at the named permission sets level, offering No Access, Read, Change, and Full Control (Special File and Directory permissions were not available).

XCACLS is a powerful and fairly complex tool, and careful reading of the associated documentation (a Word document called XCACLS.DOC in the Resource Kit directory) is advised before beginning to use it. Basic usage is as follows:

```
XCACLS <filespec> /G <user>:<permis-
sion>;<special permission>
```

This line grants <permission> to <user> for the file(s) specified in <filespec>; <special permission> applies only to directories and corresponds to the Special Directory Access settings seen in the GUI permissions.

GLOBAL And LOCAL

The NT Server Resource Kit contains more command-line tools for managing accounts. Two useful tools for reviewing group memberships are the commands GLOBAL and LOCAL, for listing the members of global and local groups respectively. The syntax is:

```
GLOBAL groupname domainname
```

or

```
GLOBAL groupname \\servername
```

The syntax for LOCAL is exactly the same. These commands list the members of the specified group, one user account per line. To review membership of a group with many members you can redirect the output of the command to a file for later examination:

```
GLOBAL groupname domainname > group-
members.txt
```

Using the above commands you can carry out administrative chores quickly rather than spend hours using the GUI equivalent tools.

For instance, you might write an automatic script to reset the security properties of users to a known base level on a regular basis. The script first dumps a list of users from a particular group to a text file, then uses NTRIGHTS and XCACLS to reset their privileges. See Figure 3.

SOON

SOON is a close relative of the AT command, whose purpose is to run a command in the near future on a local or remote machine. SOON has two distinct syntax patterns, one for running a scheduling command and one for configuring the defaults the command will use. The syntax for a scheduling command is:

```
SOON [\\COMPUTERNAME] [DELAY] [/INTER-
ACTIVE] <command>
```

If all optional parameters are omitted, and no prior configuration command has been run, <command> will be run at the local machine after a delay of five seconds, in non-interactive mode - that is, a user of the machine at the time would not see the command running or be able to interact with it.

Specify /INTERACTIVE to allow the command to interact with the desktop. DELAY can be specified on the command line, or, together with other parameters, can be set in a configuration command. The syntax of the configuration command is:

```
SOON /D [/L:N] [/R:N] [/I:{ON | OFF}]
/D
```

This, together with either /L or /N (or both), sets the default delay before a command is executed.

There are two delay parameters, /L being used to set the default delay for commands executed on the local computer and /R for commands being executed on any remote computer. In each case the delay N is specified as a whole number of seconds. The unconfigured

```
REM Log start date and time
Echo Started at >> PROGRESS.LOG
DATE /T >> PROGRESS.LOG
TIME /T >> PROGRESS.LOG
NTBACKUP <params>
DATE /T >> PROGRESS.LOG
TIME /T >> PROGRESS.LOG
Echo Finished at >> PROGRESS.LOG
```

Figure 4 - Script to find out how long a backup takes.

```
Started at
Tue 19/10/1999
22:19
<ntbackup output>
Finished at
Tue 19/10/1999
23:08
```

Figure 5 - The date and time information is split over two lines.

```
FOR /F "TOKENS=2" %%I IN ('DATE /T') DO SET MYDATE=%%I
IF EXIST DUMP.TXT DEL DUMP.TXT
DUMPEL -S \\MYSERVER -F DUMP.TXT -L SECURITY -T
RENAME DUMP.TXT %MYDATE:~8,2%%MYDATE:~3,2%%MYDATE:~0,2%SEC.TXT
```

Figure 6 - Example script showing use of DUMPEL command.

defaults are five seconds for local jobs and 15 seconds for remote jobs. The parameter /I specifies whether SOON jobs should be run interactively by default.

To set up SOON for a local delay of seven seconds and a remote delay of 11 seconds, specifying that all jobs should be interactive, use the following:

```
SOON /D /L:7 /R:11 /I:ON
```

Now call a batch script which starts the local copy of NTBACKUP on a server, starting in 11 seconds' time:

```
SOON \\MYSERVER "CMD.EXE /C
C:\SCRIPTS\STARTBACKUP.CMD"
```

SOON is both an easy interface to the AT command, and a very handy way of running a program remotely. The "correct" way to run a job remotely is to use RCMD and RCMDSVC but, for simple tasks, SOON with a very short delay gets the job done more easily.

NOW

NOW is a command I use a lot in scripts which write data to log files. If you want to find the date and time a particular action was performed (say you are interested in how long it takes to back up a particular directory), you can bookend the command which fires off NTBACKUP with commands before and afterwards to send the date and time to a file.

The NT commands DATE and TIME both have a parameter /T which suppresses the interactive prompt for a new date or time, and simply returns the current time. The appropriate code is shown in Figure 4.

However, this has the unwanted effect of splitting the date and time information over two lines, which is unorthodox and difficult to read. The contents of PROGRESS.LOG would be as shown in Figure 5.

NOW outputs the current date and time on a single line, and then appends any text that was passed to it on the command line. So,

```
NOW Started backup >> PROGRESS.LOG
```

will insert:

```
Tue Oct 19 22:20:33 1999 - Started
backup
```

into PROGRESS.LOG. My only complaint about NOW is that the date and time format is fixed, and is of little use when trying to sort or filter events in a large log composed of NOW entries. This can be worked around by using Perl to process the logs, or by pulling the log file into Excel or Access and parsing the data into columns.

DUMPEL

This command is invaluable for keeping records of NT Event Logs. It writes the contents of the designated Event Log section (System, Security or Application) out to a text file, which can then be picked up for further processing, or archived. The syntax is:

```
DUMPEL -F FILE [-S \\SERVER] -L LOG
[-M SOURCE] [-E N1 N2 N3...] [-R] [-T]
```

-F specifies the name of the file to be written out and is mandatory; it won't work without this option being specified. -S specifies the name of the server whose event log should be processed. If omitted, the current computer is assumed. You can include or omit the leading UNC slashes.

-L specifies which log is to be dumped, and the parameters are System, Security or Application. This parameter too is mandatory; if you specify an invalid log then the Application log will be dumped instead. -M is optional and lets you specify the source (ie, system component) generating a log event that you are interested in. For example, to dump only those events from the System log logged by the WINLOGON process, specify -M Winlogon.

-E allows for further filtering by Event type (the four-figure numbers that NT assigns to each system event). -R, if used with other filtering commands (-M and -E), will exclude records of the specified filter type from the log. If omitted the dump will only contain records of the type satisfying the filter conditions. -T causes the columns of the dump file to be separated with tabs (ASCII 0x9) for ease of import into a spreadsheet or database. If omitted, spaces are used as delimiters.

An example script which dumps the Security log on a daily basis to a file which is then renamed to reveal the date of the dump is shown in Figure 6.

The line calling DUMPEL is completely straightforward. However, without the rest of the batch file this would result in the dump job overwriting its output file every night. Here, the versatile FOR command is used to grab the output of DATE /T into an environment variable, which is then dissected into its components by the extended variable syntax of NT's command interpreter.

The syntax %MYDATE:~8,2% means "start at the eighth character of the contents of %MYDATE%, and take two characters"; it works rather like the function MID() in Excel or Basic. Using this syntax you can rearrange the contents of a variable and make up a meaningful file name in the form YYMMDDSEC.TXT.

Conclusion

There are 255 separate program files in the current Resource Kit utility directory tree, and the task of singling out the ten most useful ones is always going to be a difficult one. Hopefully this article has provided some idea of what can be done with the Resource Kit, and whetted your appetite to investigate other utilities as well.

PCNA

The Author

Simon Pride runs the PC support department for Cambridge University, England, and can be contacted by email as simon.pride@-itp-journals.com.

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.