Remote control

Andrew Ward looks at ways of administering your server from a distance.

A common complaint directed at Windows NT is that many of the tasks required for administering a server require that you actually sit at the server itself. Although this is true, there are a surprising number of ways to administer servers remotely. For example, many administrative tools work across the network: amongst others, Windows NT Diagnostics (winmsd), the Performance Monitor and the Event Viewer.

These tools have one thing in common: they don't allow you to do any administration because they're read-only. And, in the Unix world, utilities like Telnet, rexec and rsh allow you to readily run programs on a remote system, greatly facilitating remote administration. Clients for these services are available for Windows NT (I think they are all shipped as standard) but out-of-the box there are no corresponding services.

To solve this problem, there are many utilities provided with the Windows NT 4.0 Server Resource Kit. Since there are so many of these, it is worth looking at the capabilities and limitations of each before we look at the most interesting technique.

There are a surprising number of ways to administer remotely

Command performance

RCMD, the Remote Command service, is provided with the server version of the resource kit and provides a secure, robust way to remotely administer and run command-line programs. You'll need to install the server component, RCMDSVC.EXE, as in Fig 1. If you configure it to autostart, the service will be running whenever the system starts up, whether or not a user is logged on locally.

To open a remote session from a workstation, type RCMD, then the server name at the prompt, or put the server name on the command line, as follows:

```
rcmd \\VEGAS
```

You can also use RCMD to execute a single command by appending it to the command line, as follows:

```
rcmd \\VEGAS net stop rsh
```

You can connect up to ten clients to the remote command service on a server, and each one will operate independently of the others.

Security works in the following way. The logged-on user must have interactive log-on privileges, which you have by default, on the target computer in order to connect to it. Any programs executed on the target computer are executed as if you were logged on to the local computer itself.

The only programs which will work with RCMD are those which use STDIN, STDOUT and STDERR for input and output. This is an interesting way of discovering horrible inconsistencies with Windows NT. For example, TLIST /? will not work with RCMD although other TLIST operations do, yet NBTSTAT /? works fine. Those programs which use the Win32 Console API and MS-DOS programs will not work.

[FIG 1]

Installing the server component:

```
instsrv rcmd "c:\program files\reskit\rcmdsvc.exe"
```

[FIG 2]

To start a session, type:

```
remote /S "c:\winnt\system32\cmd.exe" sessionname
```

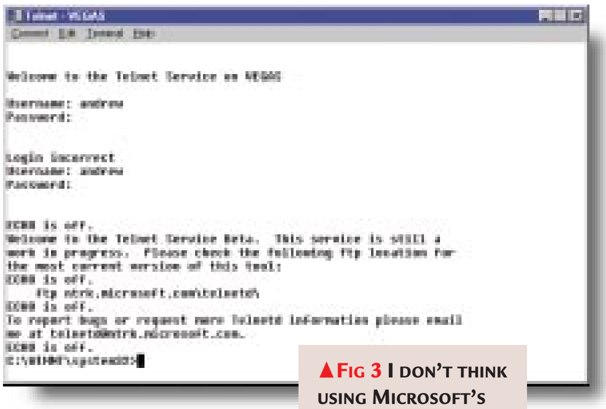
REMOTE is intended for running specific programs on a remote computer. It requires you to set up a session on the remote system for the particular command line you want to run. You can then initiate it from the client. As this involves setting up each session from the remote system, it's useless for remote administration. It is primarily intended for things like running a compiler on a remote machine to avoid loading your own processor while you get on with something else.

Starting a session

To start a session on the remote system, type the code shown in Fig 2. In this example, I've used cmd.exe as the command that will be run purely for demonstration purposes. Of course, if you do execute cmd.exe, it allows remote administration because you end up with a command window. To connect to a remote session, type:

```
remote /C VEGAS sessionname
```

REMOTE offers no security, so starting the REMOTE server leaves the system open to anyone with a remote client who knows the session name. Like RCMD, REMOTE can only be used with command-line applications.

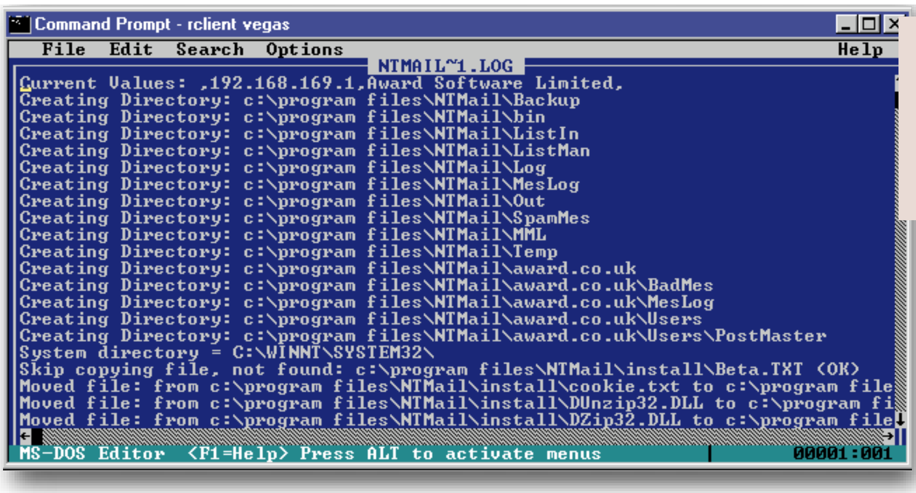


```
Welcome to the Telnet Service on VEGAS

Username: andrew
Password:


Login incorrect
Username: andrew
Password:


ECHO is off.
Welcome to the Telnet Service Beta.  This service is still a
work in progress.  Please check the following ftp location for
the most current version of this tool:
ECHO is off.
    ftp ntrk.microsoft.com/telnetd\
ECHO is off.
To report bugs or request more Telnetd information please email
me at telnetd@ntrk.microsoft.com.
ECHO is off.
C:\WINNT\system32>
```

▲Fig 3 I don't think using Microsoft's Telnet daemon beta could be classified as a rich user-experience

Telnet like it is

The point about the Telnet Server Beta provided with the resource kit is that it allows remote administration of a Windows NT system from other



```
Current Values: ,192.168.169.1,Award Software Limited,
Creating Directory: c:\program files\NTMail\Backup
Creating Directory: c:\program files\NTMail\bin
Creating Directory: c:\program files\NTMail\ListIn
Creating Directory: c:\program files\NTMail\ListMan
Creating Directory: c:\program files\NTMail\Log
Creating Directory: c:\program files\NTMail\MesLog
Creating Directory: c:\program files\NTMail\Out
Creating Directory: c:\program files\NTMail\SpamMes
Creating Directory: c:\program files\NTMail\MML
Creating Directory: c:\program files\NTMail\Temp
Creating Directory: c:\program files\NTMail\award.co.uk
Creating Directory: c:\program files\NTMail\award.co.uk\BadMes
Creating Directory: c:\program files\NTMail\award.co.uk\MesLog
Creating Directory: c:\program files\NTMail\award.co.uk\Users
Creating Directory: c:\program files\NTMail\award.co.uk\Users\PostMaster
System directory = C:\WINNT\SYSTEM32\
Skip copying file, not found: c:\program files\NTMail\install\Beta.TXT (OK)
Moved file: from c:\program files\NTMail\install\cookie.txt to c:\program file
Moved file: from c:\program files\NTMail\install\DUnzip32.DLL to c:\program fi
Moved file: from c:\program files\NTMail\install\DZip32.DLL to c:\program file
MS-DOS Editor  <F1=Help> Press ALT to activate menus            00001:001
```

◀ **Fig 4** You can even run DOS programs that carry out direct screen writes with the remote console

platforms such as Unix. Unfortunately, the beta is flaky [Fig 3, p233]. If you really want to run it, you must first install the Remote Session Manager: run the Network Control Panel, select Services, click on Add and then Have Disk, and specify c:\program files\resource kit\telnetd (or wherever you've put it); select Remote Session Manager from the list. You also need to install the Telnet service (TELNETD.EXE) in the same way.

Telnet is restricted to running command-line utilities, scripts and batch files that use STDIN, STDOUT and STDERR, but the only sure way to determine whether an application can be successfully run in a Telnet session is to try it. It is possible to run some graphical programs using Telnet; a surprise for any local computer on the server, as that is where they would pop up.

Console service

The Remote Console (Rconsole) RCLIENT application [Fig 4] works much like the others, by running a CMD session on the remote system, but the server notifies the client of changes to the video memory within the console session rather than redirecting standard output. This won't run graphical programs but it will work with command-line programs which use video memory, such as Edit.

Here's how you install the remote console service on a server. Go to the Network Control Panel and select the Services tab. Click on Add, Have Disk and specify C:\NTRESKIT\RCONSOLE if that's where you've put it. Select Remote Console Server and click OK. To run the client, type rclient and the server name:

```
rclient \\VEGAS
```

Security matters

Security receives a bit of attention with the remote console. There's a client-side command-line option to encrypt all data sent, but this only works if both ends are running Windows NT 4.0. Apart from that, the remote console client does work on other versions of Windows NT. Note that this /encrypt is not supported on the French version of Remote Console (yes, really).

[FIG 6]

Control security with this:

```
c:\winnt\system32\drivers\etc\.rhosts
```

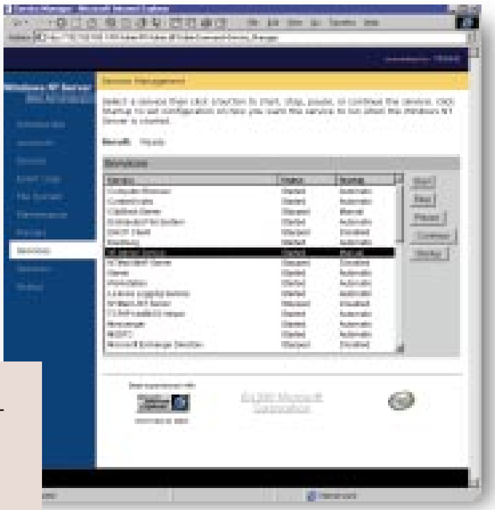
- A restriction of other remote command-line utilities is the inability to make network connections. With the remote console, a client-side command-line option /logon allows you to specify that the CMD.EXE process executed on the server has a logon ID and can make network connections. This /logon option encrypts the password sent over the network with a Data Encryption Standard (DES) algorithm if both client and server are running Windows NT 4.0.
- Because video memory changes can involve large amounts of data, rclient features an option to automatically tune the data rate to the speed of the link, say if you're connecting via RAS.
- Another security feature is that only members of the 'Administrators' group can connect to the remote console server by default. But under NT 4.0, a new group called RConsole Users is created, and you can modify its members. Administrators can always connect, regardless of how you set up this group.

Shelling out

A remote shell service, the server side of the TCP/IP utility RSH.EXE, is provided with the NT Server Resource Kit. To install the service, use the command shown in Fig 5 or as appropriate for your system. Then, start the service with this command:

```
net start rshsvc
```

Like Telnet, this allows access to a Windows NT server from a variety of different platforms, since RSH exists for nearly all major operating systems.



▶ **Fig 7** The cool way to perform remote server administration

[FIG 5]

Install a remote shell service with:

```
rshsetup "c:\program files\reskit\rshsvc.exe" "c:\program files\reskit\rshsvc.dll"
```

Security is controlled by setting up the file shown in Fig 6 (p235). Be sure to note the full-stop preceding the filename. The .rhosts file has a list of machine names followed by users from that machine who are authorised to use rsh. Rsh is not intended for use with interactive commands, and can't be used to initiate an interactive session using cmd.exe.

Web Administration

All the command-line utilities allow you to perform remote administration, but there's a learning curve involved. You have to learn what commands to type in, to perform administrative tasks. If I were paying a network administrator, I'd rather their time were spent on more productive tasks than having to memorise lists of commands. With Web Administration [Fig 7, p235], a free download from Microsoft's web site, you get an interactive graphical administrative interface that looks much like the standard control panel applets.

Before you can implement Web Administration, you need IIS 4.0 installed on the server although the minimum installation will do. (Remember to re-install your latest service pack after installing IIS 4.0 or other components from the option pack.)

To find Web Administration for Windows NT Server, go to www.microsoft.com/NTServer and select Downloads. Choose to download 'Web Administrator 2.0 for Microsoft Windows NT Server 4.0'. Once installed on the server, something that Web Administration will do for you is install the Remote Console client software. To use it, navigate to ntadmin on your server from within Internet Explorer: http://VEGAS/ntadmin.

This raises the question of why you wanted to administer the system remotely in the first place. The most common reason is because the Internet Information Server has stopped or crashed and in these circumstances Web Administration clearly isn't going to be much use.

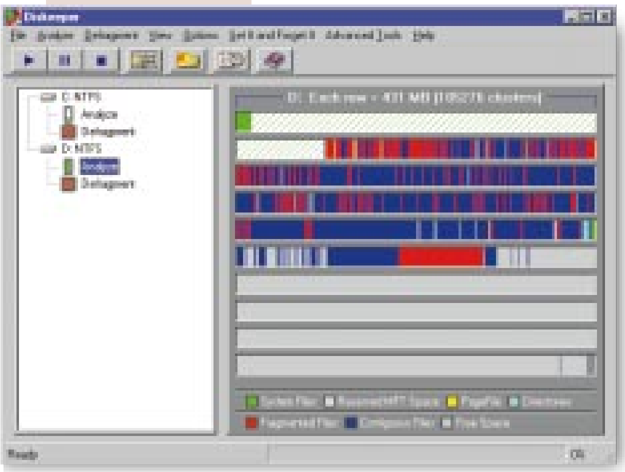
SERVER OR DOMAIN CONTROLLER?

Reader John Gresham has installed NT Server 4.0 to replace Windows 95 on a server and is naturally delighted the system is now 'working perfectly, very reliable, and no longer crashes daily as it did under Windows 95'. Yet he raises the question of whether he should have installed NT as a Primary Domain Controller (PDC) or a Standalone Server. The client systems are Windows 95 and he's installed Windows NT as a Standalone Server; hence the network is operating as a workgroup rather than a domain.

John is correct in assuming a fresh install of NT would be necessary to change the status from server to PDC, but is this necessary? Well, in his environment there's very little to choose between them, so John may as well stay with the current configuration. If the clients were NT, then a PDC would be more convenient than a server, simply in order to save having to maintain user accounts in both the workstations and the server. But this argument assumes a static environment. If the network were to become a critical computing resource, the server would need a backup, and one way to administer this arrangement would be via a PDC and a BDC (backup domain controller). Similarly, if the number of users were to increase substantially, additional servers may be necessary to handle the logon requests. You might also want to allow some granularity in granting administrative rights over departmental resources.

With Windows NT 4.0, this can be accomplished by implementing multiple domains with the appropriate trust relationships. If the workstations were to be changed to Windows NT, implementing a domain would simplify administration.

▼ Fig 8 Diskeeper 4.0 will defragment Windows NT paging files



Defrag time

Executive Software continues to find ways of improving its Diskeeper product for NT defragmentation [Fig 8]. The latest release, version 4.0, will defragment the NT paging file (version 3.0 introduced the ability to defrag and consolidate directories). If you have a maintenance contract, you're entitled to a free upgrade to Diskeeper 4.0 and by now you should have automatically received the new software. If you purchased Diskeeper for NT 3.0 after 1st September 1998 you're also entitled to a free upgrade to the new version, available from your reseller.

Diskeeper Lite, a cut-down version, is available as a free download. You can download the full product but it will expire 30 days after you have installed it. Expect to pay around £41 for a single-user copy of Diskeeper version 4.0 for Windows NT Workstation, or £213 for the Server version. To download Diskeeper Lite or a trial version of Diskeeper, visit www.execsoft.co.uk.

PerfectDisk is a better defrag tool for relatively stable systems, but on a system like my own, with frequent installation and removal of applications, upgrades, service releases, service packs and patches, Diskeeper is a much better bet.

PCW CONTACTS

Andrew Ward can be contacted via the PCW editorial office (address, p10) or email NT@pcw.co.uk