The main event

The Windows NT event logs keep track of what's happening in the system, but they themselves need regular attention. Dale Strickland-Clark shows you how they work.

When you want to know what's been happening on your system, the NT event log is the place to turn. It's the central record for notable incidents and can help with problem diagnosis, resource management and capacity planning.

Each NT workstation or server has three event logs: system, security and application. The system log contains information about configuration problems, the state of the services and the use of printers. Application programmers determine what they consider important enough for the application log and administrators control most of what is written to the security log.

These logs are a valuable source of information concerning what has happened on a system and it's a good idea to archive them daily if you're ever likely to want to examine the historical behaviour of a system.

Records are written to the event log in a format which, in part, is only understood by the application that wrote them. When you view or export the logs, the system calls upon each application to format its own records so you can make sense of them. This is great until you take a raw event log (an .EVT file) and attempt to examine it on another system. If the application that created the records isn't installed, you may find that much information won't make sense. Depending on the network, you may also find that user IDs are displayed in their internal representation, which is a curious string of digits called a SID. There is a similar danger when attempting to examine an old archived log. If applications have been removed from the system or users deleted, some log entries may reveal less than you'd like.

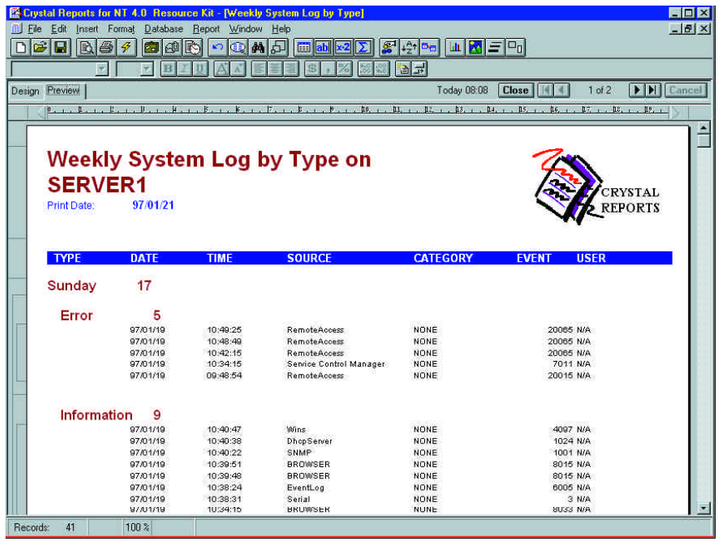
For these reasons, it's a good idea to consider the information you're likely to want to extract from event logs before choosing your storage strategy. It's also worth watching the size of the event logs you generate. Large logs of tens or even hundreds of megabytes per day on a busy system are easily achievable if you're over-zealous with auditing.

Because of the possibility of event logs becoming useless over time or losing touch with the applications creating them, long-term storage and most types of analysis are going to depend on a formatted export of the event log. I think there are three main types of uses to which the event log is put. The first is as a problem alert, although it's not really designed for this: serious problems are already written to the console and sent as messages to registered administrators. Second is as a problem diagnosis aid for when something isn't working properly and you need to find the reason. Lastly, as an audit trail, to record who's done what.

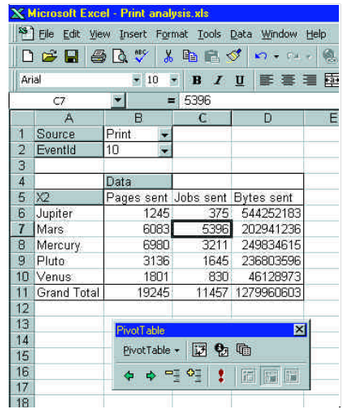
As part of a capacity planning exercise, I needed to find out which printers on a network were being most heavily used and by whom. The Event Viewer application that comes with NT is adequate for viewing raw events but pretty hopeless for analysis. While it will export the logs in a comma-delimited format, you can't automate the process and the resultant file might be described as offering an interesting challenge for analysis.

There is a tool in the NT 4 Resource Kit called DUMPEL that might have helped simplify getting the data out of the logs, but in spite of the help file suggesting otherwise, I couldn't get a comma-delimited file out of it. I'll look at this again when I come to automate the archiving of log records, but for now I was happy to get the data out by hand, using Event Viewer.

The Server version of the Resource Kit includes a copy of Crystal Reports that will read the event logs directly and produce a

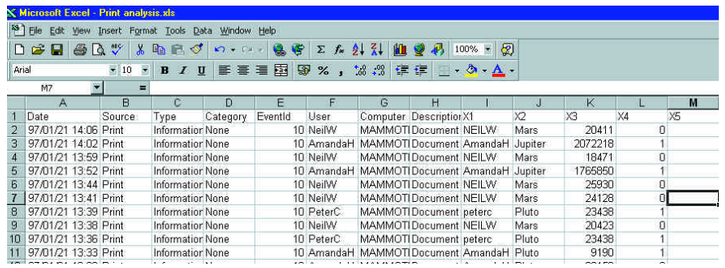


The Crystal Reports bundled in the Server Resource Kit provides exception reporting and basic analysis of event logs



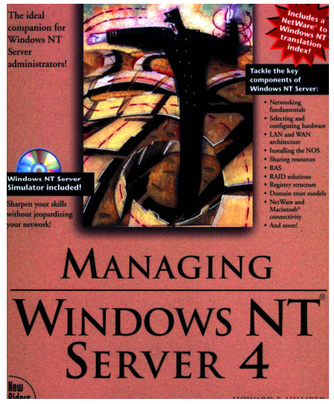
Excel's PivotTable is an ideal tool for interactive analysis. Here it summarises the use of several printers

Once the event log data has been massaged into a tidy comma-delimited format, Excel will quickly turn it into a simple database



Books

■ Managing Windows NT Server 4
Author: Howard F. Hilliker
Publisher: New Riders
Price: £46.99 (incl VAT)
This book bears a striking resemblance to *Inside Windows NT Server 4* (reviewed January 1997) by the same publisher. Many of the subjects covered are similar, and I'm also suspicious of the number "4" in the title. Parts of the text have a distinct NT 3.51 ring to them and there are even screenshots from an NT 3.51 system. Worse, the console command reference at the back of the book mentions none of the extensions introduced in NT 4. Either this is a revised 3.51 book, or it's been a long time in the making. Gripes apart, this is a solid, thorough volume covering most of the issues concerning NT administrators. The CD is a corker, with a vast amount of demonstration NT software plus a free copy of *Inside Windows NT Server* in Acrobat format.



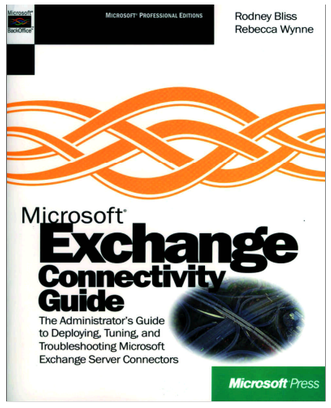
■ Whiz Bang Web Site F/X
Author: Tom Lockwood
Publisher: Que
Price: £32.99 (incl VAT)
This book solves one of the great mysteries of the web age: how do you make a background that tiles seamlessly? Also explained is using image maps, creating animated GIFs, working with audio, Java and multimedia. CGI scripts and VRML are explored along the way on the journey to producing appealing web sites.

The book adopts the unconventional approach of listing very few of the code samples on its pages, leaving you, instead, to fish them off the CD — which is nicely organised as a web site with links to relevant pages out in the real world.

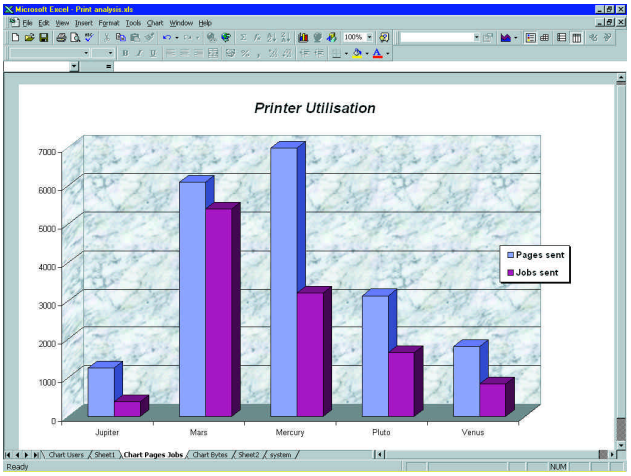
The author knows his subject well and explains it clearly. This is an ideal companion for someone already familiar with HTML but who wants to be more adventurous.

■ Microsoft Exchange Connectivity Guide
Authors: Rodney Bliss, Rebecca Wynne
Publisher: Microsoft Press
Price: £27.49 (incl VAT)
The connection possibilities offered by Exchange are many and even the experienced administrator can find themselves with a system that really should be transmitting mail but stubbornly refuses. This book explains the large number of parameters that affect message transfer and fills the very large holes left by the documentation supplied with the software. It assumes little and explains setting up a server to talk to the internet, X400 or MS Mail in networks of varying complexity.
All the dialog boxes concerned are shown and each parameter is explained along with possible problems you may encounter and what to do about them.

A very comprehensive and useful reference.



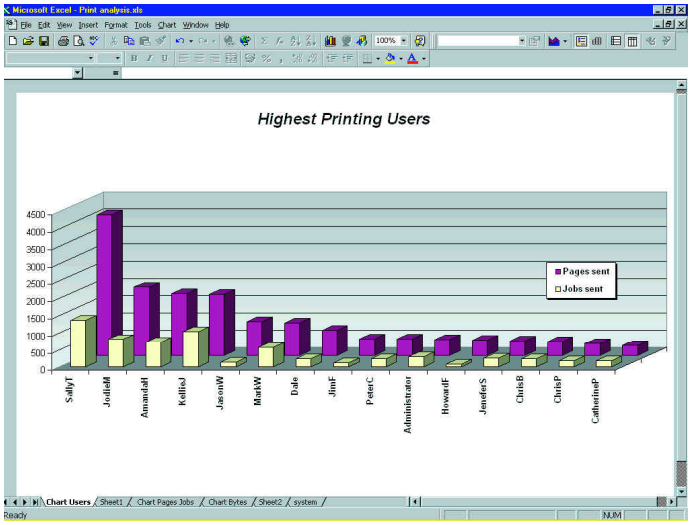
p269



Left The poor distribution of workload is now evident. Mercury, an overworked LaserJet 5P, might benefit from swapping places with Venus, a rather swift Lexmark Optra Rt+
Below Highlighting high print users might encourage economic printing behaviour. Sadly, it's turned into an ugly scramble for the top position

variety of reports, but in the end I chose Excel to do the analysis backed by a little Perl program to sanitise the data.

I exported the system log from the server into what the Event Viewer program calls a comma-delimited format and ran it through the Perl program, cleanevent.perl *(see screenshots, page 266)*. Cleanevent adds a header record, identifying the columns so Excel will treat the data as a database. It merges the date and time fields from the log, it picks up all the trailing description fields that sometimes follow a record and adds them to the end of the original record, and, finally, it identifies the records relating to printing. From these it picks out the user ID, printer name and print size, placing them in the general-purpose fields, X1 to X4, on the end of the record. If the output of cleanevent is written to a .csv file and dropped into Excel, it will automatically be split into individual cells and is immediately ready for analysis.



I called upon a PivotTable (under the Data menu) to do the analysis and finished off with a few charts to help illustrate the load on the printers.

The Perl routine could easily be extended to extract other interesting information, split the logs into smaller record sets or write it to a database for long-term analysis.

Mouse moment

If you cast your mind back to the January issue, you may recall my request that Santa deliver a new design of pointing device. Well, it wasn't Santa but Microsoft that came up with the goods, and while it's not exactly what I asked for, we're definitely heading in the right direction. I refer, of course, to Microsoft's new Intellimouse. I've only been using it a month or so and already I'm lost at a PC without one. Now, with an ordinary mouse, I find myself scraping uselessly at the little gap between the two buttons and receiving strange looks from uninitiated onlookers. Scrolling has never been so effortless. Nine out of ten points, Microsoft. I'll save the extra one for when someone comes up with a cordless version. (Are you listening, Logitech?)

PCW Contacts

Dale Strickland-Clark is a journalist and consultant on Windows/NT and the internet. He can be reached by email at NT@pcw.vnu.co.uk
Computer Manuals 0121 706 6000