NAME

readlog − text-based access to the Windows event log

SYNOPSIS

readlog [**−t** *fmt*] [**−v** *srv*] [**−riuwsycabdn**] [*source* ...]

DESCRIPTION

Readlog provides text-based access to the Windows event log. It can thus be used to textually process the data that is normaly seen through the Windows *event viewer* program. Running *readlog* without any options will generate a listing of the *System* event log in a format remininscent of the Unix *syslogd* log files such as the following:

Apr 20 08:35:28 SEAGULL Srv: -: Warning: The C: disk is at or near capacity. You may need to delete some files.

By default each entry contains the time, the computer name, the application name, the log message category (where available), the log message type (error, warning, information, audit success, or audit failure), and the the error message. Under Windows the event log does not contain the actual messages, but pointers to files that contain pre-compiled message strings. Failure to obtain such a message string will result in an error message, but *readlog* will continue its operation displaying the message code.

Without any parameters *readlog* will print the contents of the *System* event log. Windows systems typically also contain *Application* and *Security* logs. In addition, applications can install other custom log files. You can see the files available on your system in the registry under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog branch. One or more event log files can be specified as arguments to *readlog*.

OPTIONS

−f fmt Specify the format to display the event generation time using the *strftime(3)* escape sequences.

−v src Specify the server name from which to obtain the event log as a UNC name.

−r Print entries in reverse chronological order starting from the latest entry and going back in time.

−i Output the decimal event id.

−u Do not print user information; normally user information is printed using the *domain\user* convention.

−w Do not print the workstation name.

−s Do not print the event source.

−y Do not print the event type.

−c Do not print the event category (most events have no categories registered, so you will in many cases just see a single dash).

−a Output event-specific data as ASCII.

−b Output event-specific data as hex bytes.

−d Output event-specific data as hex doublewords.

−n Format event using newline separators; normally each event is displayed in a single line.

EXAMPLE

readlog | grep "The Event log service was started" | wc -l
can be used to count the number of system boots registered in the log.

readlog Application | awk -F: "/Outbound: Information: Fax Sent/{print $12}" | sort | uniq -c | sort -rn
Create an list of fax recipients ordered by the number of faxes they have received.

SEE ALSO

D. Spinellis. Outwit: Unix tool-based programming meets the Windows world. In *USENIX 2000 Technical Conference Proceedings*, pages 149-158, San Diego, CA, USA, June 2000, USENIX Association.
Microsoft Corporation. *Microsoft Windows NT Server 4.0 Resource Kit*. Microsoft Press.

AUTHOR

BUGS

Remote system access has not been tested.

Windows event log messages are sometimes difficult to parse using text-based tools.