NAME

eventlogadm - push records into the Samba event log store

SYNOPSIS

eventlogadm [**-s**] [**-d**] [**-h**] **-o** addsource *EVENTLOG SOURCENAME MSGFILE*

eventlogadm [**-s**] [**-d**] [**-h**] **-o** write *EVENTLOG*

eventlogadm [**-s**] [**-d**] [**-h**] **-o** dump *EVENTLOG RECORD_NUMBER*

DESCRIPTION

This tool is part of the **samba**(1) suite.

eventlogadm is a filter that accepts formatted event log records on standard input and writes them to the Samba event log store. Windows client can then manipulate these record using the usual administration tools.

OPTIONS

-s *FILENAME*

The -s option causes eventlogadm to load the configuration file given as FILENAME instead of the default one used by Samba.

-d

The -d option causes eventlogadm to emit debugging information.

-o addsource *EVENTLOG SOURCENAME MSGFILE*

The -o addsource option creates a new event log source.

-o write *EVENTLOG*

The -o write reads event log records from standard input and writes them to the Samba event log store named by EVENTLOG.

-o dump *EVENTLOG RECORD_NUMBER*

The -o dump reads event log records from a EVENTLOG tdb and dumps them to standard output on screen.

-h

Print usage information.

EVENTLOG RECORD FORMAT

For the write operation, eventlogadm expects to be able to read structured records from standard input. These records are a sequence of lines, with the record key and data separated by a colon character. Records are separated by at least one or more blank line.

The event log record field are:

•
- This field should be 0, since eventlogadm will calculate this value.

•
- This must be the value 1699505740.

•
- This field should be 0.

•
- The time the eventlog record was generated; format is the number of seconds since 00:00:00 January 1, 1970, UTC.

•
- The time the eventlog record was written; format is the number of seconds since 00:00:00 January 1, 1970, UTC.

•
- The eventlog ID.

•
- The event type -- one of "INFO", "ERROR", "WARNING", "AUDIT SUCCESS" or "AUDIT FAILURE".

•
- The event category; this depends on the message file. It is primarily used as a means of filtering in the eventlog viewer.

•
- This field should be 0.

•
- This field should be 0.

⊕

- This field should be 0.

⊕

- This field contains the source name associated with the event log. If a message file is used with an event log, there will be a registry entry for associating this source name with a message file DLL.

⊕

- The name of the machine on which the eventlog was generated. This is typically the host name.

⊕

- The text associated with the eventlog. There may be more than one string in a record.

⊕

- This field should be left unset.

EXAMPLES

An example of the record format accepted by eventlogadm:

```
LEN: 0
RS1: 1699505740
RCN: 0
TMG: 1128631322
TMW: 1128631322
EID: 1000
ETP: INFO
ECT: 0
RS2: 0
CRN: 0
USL: 0
SRC: cron
SRN: dmlinux
STR: (root) CMD ( rm -f /var/spool/cron/lastrun/cron.hourly)
DAT:
```

Set up an eventlog source, specifying a message file DLL:

```
eventlogadm -o addsource Application MyApplication | \\
        %SystemRoot%/system32/MyApplication.dll
```

Filter messages from the system log into an event log:

```
tail -f /var/log/messages | \\
        my_program_to_parse_into_eventlog_records | \\
        eventlogadm SystemLogEvents
```

VERSION

This man page is part of version 4.13.17 of the Samba suite.

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.