NAME

auditstat – display kernel audit statistics

SYNOPSIS

auditstat [**-c** *count*] [**-h** *numlines*] [**-i** *interval*] [**-n**] [**-v**]

AVAILABILITY

The functionality described in this man page is available only if the Basic Security Module (BSM) has been enabled. See **bsmconv**(1M) for more information.

DESCRIPTION

auditstat displays kernel audit statistics. The fields displayed are as follows:

aud
The total number of audit records processed by the **audit**(2) system call.

ctl
This field is obsolete.

drop
The total number of audit records that have been dropped. Records are dropped according to the kernel audit policy. See **auditon**(2), AUDIT_CNT policy for details.

enq
The total number of audit records put on the kernel audit queue.

gen
The total number of audit records that have been constructed (not the number written).

kern
The total number of audit records produced by user processes (as a result of system calls).

mem
The total number of Kbytes of memory currently in use by the kernel audit module.

nona
The total number of non-attributable audit records that have been constructed. These are audit records that are not attributable to any particular user.

rblk
The total number of times that **auditsvc**(2) has blocked waiting to process audit data.

tot
The total number of Kbytes of audit data written to the audit trail.

wblk
The total number of times that user processes blocked on the audit queue at the high water mark.

wrtn
The total number of audit records written. The difference between **enq** and **wrtn** is the number of outstanding audit records on the audit queue that have not been written.

OPTIONS

-c *count*
Display the statistics a total of *count* times. If *count* is equal to zero, statistics are displayed indefinitely. A time interval must be specified.

-h *numlines*
Display a header for every *numlines* of statistics printed. The default is to display the header every 20 lines. If *numlines* is equal to zero, the header is never displayed.

-i *interval*
Display the statistics every *interval* where *interval* is the number of seconds to sleep between each collection.

-n
Display the number of kernel audit events currently configured.

-v
Display the version number of the kernel audit module software.

ERRORS

auditstat returns 0 upon success and 1 upon failure.

SEE ALSO

auditconfig(1M), **praudit**(1M), **bsmconv**(1M), **audit**(2), **auditon**(2), **auditsvc**(2)