NAME

getacinfo, getacdir, getacflg, getacmin, getacna, setac, endac – get audit control file information

SYNOPSIS

cc [*flag* ...] *file* ... **–lbsm –lsocket –lnsl –lintl** [*library* ...]

#include <bsm/libbsm.h>

int getacdir(char **dir,* **int** *len***);**

int getacmin(int **min_val***);**

int getacflg(char **auditstring,* **int** *len***);**

int getacna(char **auditstring,* **int** *len***);**

void setac(void);

void endac(void);

MT-LEVEL

Safe.

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

When first called, **getacdir( )** provides information about the first audit directory in the **audit_control** file; thereafter, it returns the next directory in the file. Successive calls list all the directories listed in **audit_control**(4) The parameter *len* specifies the length of the buffer *dir*. On return, *dir* points to the directory entry.

getacmin( ) reads the minimum value from the **audit_control** file and returns the value in **min_val**. The minimum value specifies how full the file system to which the audit files are being written can get before the script **audit_warn**(1M) is invoked.

getacflg( ) reads the system audit value from the **audit_control** file and returns the value in *auditstring*. The parameter *len* specifies the length of the buffer *auditstring*.

getacna( ) reads the system audit value for non-attributable audit events from the **audit_control** file and returns the value in *auditstring*. The parameter *len* specifies the length of the buffer *auditstring*. Non-attributable events are events that cannot be attributed to an individual user. **inetd**(1M) and several other daemons record non-attributable events.

Calling *setac* rewinds the **audit_control** file to allow repeated searches.

Calling *endac* closes the **audit_control** file when processing is complete.

FILES

/etc/security/audit_control contains default parameters read by the audit daemon, **auditd**(1M)

RETURN VALUES

getacdir( ), **getacflg( )**, **getacna( )** and **getacmin( )** return:

0 on success.

–**2** on failure and set **errno** to indicate the error.

getacmin( ) and **getacflg( )** return:

1 on EOF.

getacdir( ) returns:

–**1** on EOF.

2 if the directory search had to start from the beginning because one of the other functions was called between calls to **getacdir( )**.

These functions return:

–**3** if the directory entry format in the **audit_control** file is incorrect.

getacdir( ), **getacflg( )** and **getacna( )** return:

–**3** if the input buffer is too short to accommodate the record.

SEE ALSO

audit_warn(1M), **bsmconv**(1M), **inetd**(1M), **audit_control**(4)