NAME

setac, **endac**, **getacdir**, **getacdist**, **getacexpire**, **getacfilesz**, **getacflg**, **getachost**, **getacmin**, **getacna**, **getacpol**, **au_poltostr**, **au_strtopol** - look up information from the audit_control database

LIBRARY

Basic Security Module Library (libbsm, -lbsm)

SYNOPSIS

#include <bsm/libbsm.h>

void
setac(*void*);

void
endac(*void*);

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

int
getacdist(*void*);

int
getacexpire(*int *andflg, time_t *age, size_t *size*);

int
getacfilesz(*size_t *size_val*);

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

int
getachost(*char *auditstr, int len*);

int
getacmin(*int *min_val*);

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

int
getacpol(*char *auditstr, size_t len*);

int
getacqsize(*int *size_val*);

ssize_t
au_poltostr(*int policy, size_t maxsize, char *buf*);

int
au_strtopol(*const char *polstr, int *policy*);

DESCRIPTION

These interfaces may be used to look up information from the audit_control(5) database, which contains various audit-related administrative parameters.

The **setac**() function resets the database iterator to the beginning of the database; see the *BUGS* section for more information.

The **endac**() function closes the audit_control(5) database.

The **getacdir**() function returns the name of the directory where log data is stored via the passed character buffer *name* of length *len*.

The **getacdist**() function returns a value that allows to decide if trail files distribution is turned on or off.

The **getacexpire**() function returns the audit trail file expiration parameters in the passed *int* buffer *andflg*, *time_t* buffer *age* and *size_t* buffer *size*. If the parameter is not specified in the audit_control(5) file it is set to zero.

The **getacfilesz**() function returns the audit trail rotation size in the passed *size_t* buffer *size_val*.

The **getacflg**() function returns the audit system flags via the the passed character buffer *auditstr* of length *len*.

The **getachost**() function returns the local systems's audit host information via the the passed character buffer *auditstr* of length *len*.

The **getacmin**() function returns the minimum free disk space for the audit log target file system via the passed *min_val* variable.

The **getacna**() function returns the non-attributable flags via the passed character buffer *auditstr* of length *len*.

The **getacpol**() function returns the audit policy flags via the passed character buffer *auditstr* of length *len*.

The **getacqsize**() function returns the size of the audit post-commit queue in the passed *size_val* buffer. If the parameter is not specified in the audit_control(5) file it is set to -1, indicating that the kernel's default queue size is being used.

The **au_poltostr**() function converts a numeric audit policy mask, *policy*, to a string in the passed character buffer *buf* of lenth *maxsize*.

The **au_strtopol**() function converts an audit policy flags string, *polstr*, to a numeric audit policy mask returned via *policy*.

RETURN VALUES

The **getacfilesz**(), **getacdir**(), **getacexpire**(), **getacflg**(), **getachost**(), **getacmin**(), **getacna**(), **getacpol**(), **getacqsize**(), and **au_strtopol**() functions return 0 on success, or a negative value on failure, along with error information in *errno*.

The **au_poltostr**() function returns a string length of 0 or more on success, or a negative value on if there is a failure.

The **getacdist**() function returns 1 if trail files distribution is turned on, 0 if it is turned off or negative value on failure.

Functions that return a string value will return a failure if there is insufficient room in the passed character buffer for the full string.

SEE ALSO

libbsm(3), audit_control(5)

HISTORY

The OpenBSM implementation was created by McAfee Research, the security division of McAfee Inc., under contract to Apple Computer, Inc., in 2004. It was subsequently adopted by the TrustedBSD Project as the foundation for the OpenBSM distribution.

AUTHORS

This software was created by Robert Watson, Wayne Salamon, and Suresh Krishnaswamy for McAfee

Research, the security research division of McAfee, Inc., under contract to Apple Computer, Inc.

The Basic Security Module (BSM) interface to audit records and audit event stream format were defined by Sun Microsystems.

BUGS

These routines cannot currently distinguish between an entry not being found and an error accessing the database. The implementation should be changed to return an error via *errno* when NULL is returned.

There is no reason for the **setac**() interface to be exposed as part of the public API, as it is called implicitly by other access functions and iteration is not supported.

These interfaces inconsistently return various negative values depending on the failure mode, and do not always set *errno* on failure.