NAME

au_preselect – preselect an audit event

SYNOPSIS

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

#include <bsm/libbsm.h>

int au_preselect(au_event_t *event*, **au_mask_t** **mask_p*, **int** *sorf*, **int** *flag***);**

MT_LEVEL

MT-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

au_preselect( ) determines whether or not the audit event *event* is preselected against the binary preselection mask pointed to by *mask_p* (usually obtained by a call to **getaudit**(2)). **au_preselect( )** looks up the classes associated with *event* in **audit_event**(4) and compares them with the classes in *mask_p*. If the classes associated with *event* match the classes in the specified portions of the binary preselection mask pointed to by *mask_p*, the event is said to be preselected.

sorf indicates whether the comparison is made with the success portion, the failure portion or both portions of the mask pointed to by *mask_p*.

The following are the valid values of *sorf*:

AU_PRS_SUCCESS
Compare the event class with the success portion of the preselection mask.

AU_PRS_FAILURE
Compare the event class with the failure portion of the preselection mask.

AU_PRS_BOTH
Compare the event class with both the success and failure portions of the preselection mask.

flag tells **au_preselect( )** how to read the **audit_event**(4) database. Upon initial invocation, **au_preselect( )** reads the **audit_event**(4) database and allocates space in an internal cache for each entry with **malloc**(3C). In subsequent invocations, the value of *flag* determines where **au_preselect()** obtains audit event information. The following are the valid values of *flag*:

AU_PRS_REREAD
Get audit event information by searching the **audit_event**(4) database.

AU_PRS_USECACHE
Get audit event information from internal cache created upon the initial invocation. This option is much faster.

RETURN VALUES

au_preselect( ) returns:

- **0** *event* is not preselected.
- **1** *event* is preselected.
- **-1** An error occurred. **au_preselect( )** couldn't allocate memory or couldn't find *event* in the **audit_event**(4) database.

FILES

/etc/security/audit_class maps audit class number to audit class names and descriptions

/etc/security/audit_event maps audit even number to audit event names and associates

SEE ALSO

bsmconv(1M), **getaudit**(2), **au_open**(3), **getauclassent**(3), **getauevent**(3), **malloc**(3C), **audit_class**(4), **audit_event**(4)

NOTES

au_preselect( ) is normally called prior to constructing and writing an audit record. If the event is not preselected, the overhead of constructing and writing the record can be saved.