NAME

auditon – manipulate auditing

SYNOPSIS

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

#include <sys/param.h>
#include <bsm/audit.h>

int auditon(int *cmd***, caddr_t** *data***, int** *length***);**

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

The **auditon** system call performs various audit subsystem control operations. The *cmd* argument designates the particular audit control command. The *data* argument is a pointer to command specific data. The *length* argument is the length in bytes of the command specific data.

The following commands are supported:

A_GETCOND
Returns the system audit on/off/disabled condition in the integer long pointed to by *data.*

A_SETCOND
Sets the system's audit on/off condition to the value in the integer long pointed to by *data.* If the current state is disabled, the BSM audit module must be enabled by **bsmconv**(1M) before auditing can be turned on.

A_GETCLASS
Returns the event to class mapping for the designated audit event. The *data* argument points to the **au_evclass_map** structure containing the event number. The preselection class mask is returned in the same structure.

A_SETCLASS
Sets the event class preselection mask for the designated audit event. The *data* argument points to the **au_evclass_map** structure containing the event number and class mask.

A_GETKMASK
Returns the kernel preselection mask in the **au_mask** structure pointed to by *data.*

A_SETKMASK
Sets the kernel preselection mask. The *data* argument points to the **au_mask** structure containing the class mask.

A_GETPINFO
Returns the audit ID, preselection mask, terminal ID and audit session ID of the specified process in the **auditpinfo** structure pointed to by *data.*

A_SETPMASK
Sets the preselection mask of the specified process. The *data* argument points to the **auditpinfo** structure containing the process ID and the preselection mask.

A_SETUMASK
Sets the preselection mask for all processes with the specified audit ID. The *data* argument points to the **auditinfo** structure containing the audit ID and the preselection mask.

A_SETSMASK
Sets the preselection mask for all processes with the specified audit session ID. The *data* argument points to the **auditinfo** structure containing the audit session ID and the preselection mask.

A_GETQCTRL
Returns the kernel audit queue control parameters. These control the high and low water marks of the number of audit records allowed in the audit queue. Another parameter controls the size of the data buffer used by **auditsvc**(2) to write data to the audit trail. There is also a parameter that specifies a delay before data is written to the audit trail. The audit queue parameters are returned in the **au_qctrl** structure pointed to by *data.*

A_SETQCTRL
Sets the kernel audit queue control parameters. The *data* argument points to the **au_qctrl** structure containing the audit queue control parameters.

A_GETCWD
Returns the current working directory as kept by the audit subsystem. This is a path anchored on the real root, rather than on the active root. The *data* argument points to a buffer into which the path is copied. The *length* argument provides the length of the buffer.

A_GETCAR
Returns the current active root as kept by the audit subsystem. This path may be used to anchor an absolute path for a path token generated by an application. The *data* argument points to a buffer into which the path is copied. The *length* argument provides the length of the buffer.

A_GETSTAT
Returns the system audit statistics in the **audit_stat** structure pointed to by *data.*

A_SETSTAT
Resets system audit statistics values.

A_GETPOLICY
Returns the audit policy flags in the integer long pointed to by *data.*

A_SETPOLICY
Sets the audit policy flags to the values in the integer long pointed to by *data.* The following policy flags are recognized:

AUDIT_CNT Do not suspend processes when audit storage is full or inaccessible. The default action is to suspend processes until storage becomes available.

AUDIT_ARGV Include the argument list for the **exec**(2) system call in the audit record. The default action is not to include this information.

AUDIT_ARGE Include the environment variables for the **execv**(2) system call in the audit record. The default action is not to include this information.

AUDIT_SEQ Add a *sequence* token to each audit record. The default action is not to include it.

AUDIT_TRAIL Append a *trailer* token to each audit record. The default action is not to include it.

AUDIT_GROUP
Include the supplementary groups list in audit records. The default action is not to include it.

AUDIT_PATH Include secondary paths in audit records. Examples of secondary paths are dynamically loaded shared library modules and the command shell path for executable scripts.

Only the super-user may successfully execute this call.

RETURN VALUES

auditon( ) returns:

0 on success.

–1 on failure and sets **errno** to indicate the error.

ERRORS

EFAULT The copy of data to/from the kernel failed.

EINVAL One of the system call arguments was illegal.

EPERM The process's effective user ID is not super-user.

SEE ALSO

auditd(1M), **bsmconv**(1M), **audit**(2), **auditsvc**(2), **audit.log**(4)