NAME

audit_warn – audit daemon warning script

SYNOPSIS

/etc/security/audit_warn [*option* [*arguments*]]

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 **audit_warn** script processes warning or error messages from the audit daemon. When a problem is encountered, the audit daemon, **auditd**(1M) calls **audit_warn** with the appropriate arguments. The *option* argument specifies the error type.

The system administrator can specify a list of mail recipients to be notified when an audit_warn situation arises by defining a mail alias called *audit_warn* in **aliases**(4). The users that make up the *audit_warn* alias are typically the **audit** and **root** users.

OPTIONS

allhard *count*
: Indicates that the hard limit for all filesystems has been exceeded *count* times. The default action for this option is to send mail to the *audit_warn* alias only if the *count* is **1**, and to write a message to the machine console every time. It is recommended that mail *not* be sent every time as this could result in a the saturation of the file system that contains the mail spool directory.

allsoft
: Indicates that the soft limit for all filesystems has been exceeded. The default action for this option is to send mail to the *audit_warn* alias and to write a message to the machine console.

auditoff
: Indicates that someone other than the audit daemon changed the system audit state to something other than **AUC_AUDITING**. The audit daemon will have exited in this case. The default action for this option is to send mail to the *audit_warn* alias and to write a message to the machine console.

ebusy
: Indicates that the audit daemon is already running. The default action for this option is to send mail to the *audit_warn* alias and to write a message to the machine console.

getacdir *count*
: Indicates that there is a problem getting the directory list from **audit_control**(4). The audit daemon will hang in a sleep loop until the file is fixed. The default action for this option is to send mail to the *audit_warn* alias only if *count* is **1**, and to write a message to the machine console every time. It is recommended that mail *not* be sent every time as this could result in a the saturation of the file system that contains the mail spool directory.

hard *filename*
Indicates that the hard limit for the file has been exceeded. The default action for this option is to send mail to the *audit_warn* alias and to write a message to the machine console.

nostart
Indicates that auditing could not be started. The default action for this option is to send mail to the *audit_warn* alias and to write a message to the machine console. Some administrators may prefer to modify *audit_warn* to reboot the system when this error occurs.

postsigterm
Indicates that an error occurred during the orderly shutdown of the audit daemon. The default action for this option is to send mail to the *audit_warn* alias and to write a message to the machine console.

soft *filename*
Indicates that the soft limit for *filename* has been exceeded. The default action for this option is to send mail to the *audit_warn* alias and to write a message to the machine console.

tmpfile
Indicates that the temporary audit file already exists indicating a fatal error. The default action for this option is to send mail to the *audit_warn* alias and to write a message to the machine console.

SEE ALSO

audit(1M), **auditd**(1M), **bsmconv**(1M), **aliases**(4), **audit.log**(4), **audit_control**(4)