NAME

auditd – audit daemon

SYNOPSIS

/usr/sbin/auditd

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 daemon controls the generation and location of audit trail files. If auditing is desired, **auditd** reads the **audit_control**(4) file to get a list of directories into which audit files can be written and the percentage limit for how much space to reserve on each filesystem before changing to the next directory.

If **auditd** receives the signal **SIGUSR1**, the current audit file is closed and another is opened. If **SIGHUP** is received, the current audit trail is closed, the **audit_control** file reread, and a new trail is opened. If **SIGTERM** is received, the audit trail is closed and auditing is terminated. The program **audit**(1M) sends these signals and is recommended for this purpose.

Each time the audit daemon opens a new audit trail file, it updates the file **audit_data**(4) to include the correct name.

Auditing Conditions

The audit daemon invokes the program **audit_warn**(1M) under the following conditions with the indicated options:

audit_warn soft *pathname*
The file system upon which *pathname* resides has exceeded the minimum free space limit defined in **audit_control**(4). A new audit trail has been opened on another file system.

audit_warn allsoft
All available file systems have been filled beyond the minimum free space limit. A new audit trail has been opened anyway.

audit_warn hard *pathname*
The file system upon which *pathname* resides has filled or for some reason become unavailable. A new audit trail has been opened on another file system.

audit_warn allhard *count*
All available file systems have been filled or for some reason become unavailable. The audit daemon will repeat this call to **audit_warn** every twenty seconds until space becomes available. *count* is the number of times that **audit_warn** has been called since the problem arose.

audit_warn ebusy
There is already an audit daemon running.

audit_warn tmpfile
The file **/etc/security/audit/audit_tmp** exists, indicating a fatal error.

audit_warn nostart
The internal system audit condition is **AUC_FCHDONE**. Auditing cannot be started without rebooting the system.

audit_warn auditoff
The internal system audit condition has been changed to not be **AUC_AUDITING** by someone other than the audit daemon. This causes the audit daemon to exit.

audit_warn postsigterm
An error occurred during the orderly shutdown of the auditing system.

audit_warn getacdir
There is a problem getting the directory list from **/etc/security/audit/audit_control**.

The audit daemon will hang in a sleep loop until this file is fixed.

FILES

/etc/security/audit/audit_control
/etc/security/audit/audit_data

SEE ALSO

audit(1M), **audit_warn**(1M), **bsmconv**(1M), **praudit**(1M), **auditon**(2), **auditsvc**(2), **audit.log**(4), **audit_control**(4), **audit_data**(4)