NAME

audit - audit management utility

SYNOPSIS

audit -e | **-i** | **-n** | **-s** | **-t**

DESCRIPTION

The **audit** utility controls the state of the audit system. One of the following flags is required as an argument to **audit**:

-e Forces the audit system to immediately remove audit log files that meet the expiration criteria specified in the audit control file without doing a log rotation.

-i Initializes and starts auditing. This option is currently for Mac OS X only and requires auditd(8) to be configured to run under launchd(8).

-n Forces the audit system to close the existing audit log file and rotate to a new log file in a location specified in the audit control file. Also, audit log files that meet the expiration criteria specified in the audit control file will be removed.

-s Specifies that the audit system should [re]synchronize its configuration from the audit control file. A new log file will be created.

-t Specifies that the audit system should terminate. Log files are closed and renamed to indicate the time of the shutdown.

NOTES

The auditd(8) daemon must already be running. Optionally, it can be configured to be started on-demand by launchd(8) (Mac OS X only). The **audit** utility requires audit administrator privileges for successful operation.

FILES

/etc/security/audit_control Audit policy file used to configure the auditing system.

SEE ALSO

audit(4), audit_control(5), auditd(8), launchd(8) (Mac OS X)

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 McAfee Research, the security research division of McAfee, Inc., under contract to Apple Computer Inc. Additional authors include Wayne Salamon, Robert Watson, and SPARTA Inc.

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