NAME

auditd - audit log management daemon

SYNOPSIS

auditd [**-d** | **-l**]

DESCRIPTION

The **auditd** daemon responds to requests from the audit(8) utility and notifications from the kernel. It manages the resulting audit log files and specified log file locations.

The options are as follows:

-d Starts the daemon in debug mode -- it will not daemonize.

-l This option is for when **auditd** is configured to start on-demand using launchd(8).

Optionally, the audit review group "audit" may be created. Non-privileged users that are members of this group may read the audit trail log files.

NOTE

To assure uninterrupted audit support, the **auditd** daemon should not be started and stopped manually. Instead, the audit(8) command should be used to inform the daemon to change state/configuration after altering the *audit_control* file.

If **auditd** is started on-demand by launchd(8) then auditing should only be started and stopped with audit(8).

On Mac OS X, **auditd** uses the asl(3) API for writing system log messages. Therefore, only the audit administrator and members of the audit review group will be able to read the system log entries.

FILES

/var/audit Default directory for storing audit log files.

/etc/security The directory containing the auditing configuration files audit_class(5), audit_control(5), audit_event(5), and audit_warn(5).

COMPATIBILITY

The historical **-h** and **-s** flags are now configured using audit_control(5) policy flags **ahlt** and **cnt**, and are no longer available as arguments to **auditd**.

SEE ALSO

asl(3), audit(4), audit_class(5), audit_control(5), audit_event(5), audit_warn(5), audit(8), auditdistd(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.