NAME

audit - Security Event Audit

SYNOPSIS

options AUDIT

DESCRIPTION

Security Event Audit is a facility to provide fine-grained, configurable logging of security-relevant events, and is intended to meet the requirements of the Common Criteria (CC) Common Access Protection Profile (CAPP) evaluation. The FreeBSD **audit** facility implements the de facto industry standard BSM API, file formats, and command line interface, first found in the Solaris operating system. Information on the user space implementation can be found in libbsm(3).

Audit support is enabled at boot, if present in the kernel, using an rc.conf(5) flag. The audit daemon, auditd(8), is responsible for configuring the kernel to perform **audit**, pushing configuration data from the various audit configuration files into the kernel.

Audit Special Device

The kernel **audit** facility provides a special device, */dev/audit*, which is used by auditd(8) to monitor for **audit** events, such as requests to cycle the log, low disk space conditions, and requests to terminate auditing. This device is not intended for use by applications.

Audit Pipe Special Devices

Audit pipe special devices, discussed in auditpipe(4), provide a configurable live tracking mechanism to allow applications to tee the audit trail, as well as to configure custom preselection parameters to track users and events in a fine-grained manner.

DTrace Audit Provider

The DTrace Audit Provider, dtaudit(4), allows D scripts to enable capture of in-kernel audit records for kernel audit event types, and then process their contents during audit commit or BSM generation.

SEE ALSO

auditreduce(1), praudit(1), audit(2), auditctl(2), auditon(2), getaudit(2), getauid(2), poll(2), select(2), setaudit(2), setauid(2), libbsm(3), auditpipe(4), dtaudit(4), audit.log(5), audit_class(5), audit_control(5), audit_event(5), audit_user(5), audit_warn(5), rc.conf(5), audit(8), auditd(8), auditdistd(8)

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.

Support for kernel **audit** first appeared in FreeBSD 6.2.

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.

This manual page was written by Robert Watson <*rwatson@FreeBSD.org*>.

BUGS

The FreeBSD kernel does not fully validate that audit records submitted by user applications are syntactically valid BSM; as submission of records is limited to privileged processes, this is not a critical bug.

Instrumentation of auditable events in the kernel is not complete, as some system calls do not generate audit records, or generate audit records with incomplete argument information.

Mandatory Access Control (MAC) labels, as provided by the mac(4) facility, are not audited as part of records involving MAC decisions.

Currently the **audit** syscalls are not supported for jailed processes. However, if a process has **audit** session state associated with it, audit records will still be produced and a zonename token containing the jail’s ID or name will be present in the audit records.