NAME

audit_user - events to be audited for given users

DESCRIPTION

The **audit_user** file specifies which audit event classes are to be audited for the given users. If specified, these flags are combined with the system-wide audit flags in the audit_control(5) file to determine which classes of events to audit for that user. These settings take effect when the user logs in.

Each line maps a user name to a list of classes that should be audited and a list of classes that should not be audited. Entries are of the form:

username:*alwaysaudit*:*neveraudit*

In the format above, *alwaysaudit* is a set of event classes that are always audited, and *neveraudit* is a set of event classes that should not be audited. These sets can indicate the inclusion or exclusion of multiple classes, and whether to audit successful or failed events. See audit_control(5) for more information about audit flags.

Example entries in this file are:

```
root:lo,ad:no
jdoe:-fc,ad:+fw
```

These settings would cause login/logout and administrative events that are performed on behalf of user "root" to be audited. No failure events are audited. For the user "jdoe", failed file creation events are audited, administrative events are audited, and successful file write events are never audited.

IMPLEMENTATION NOTES

Per-user and global audit preselection configuration are evaluated at time of login, so users must log out and back in again for audit changes relating to preselection to take effect.

Audit record preselection occurs with respect to the audit identifier associated with a process, rather than with respect to the UNIX user or group ID. The audit identifier is set as part of the user credential context as part of login, and typically does not change as a result of running setuid or setgid applications, such as su(1). This has the advantage that events that occur after running su(1) can be audited to the original authenticated user, as required by CAPP, but may be surprising if not expected.

FILES

/etc/security/audit_user

SEE ALSO

login(1), su(1), audit(4), audit_class(5), audit_control(5), audit_event(5)

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.