NAME

auditconfig – configure auditing

SYNOPSIS

auditconfig [*args*]

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

auditconfig provides a command line interface to get and set kernel audit parameters.

OPTIONS

-chkconf Check the configuration of kernel audit event to class mappings. If the runtime class mask of a kernel audit event does not match the configured class mask, a mismatch is reported.

-conf Configure kernel audit event to class mappings. Runtime class mappings are changed to match those in the audit event to class database file.

-getcond Display the kernel audit condition. The condition displayed is the literal string **auditing** meaning auditing is enabled and turned on (the kernel audit module is constructing and queuing audit records) or **noaudit** meaning auditing is enabled but turned (the kernel audit module is not constructing and queuing audit records), or **disabled** meaning that the audit module has not been enabled. See **auditon**(2) and **auditd**(1M) for further information.

-setcond[auditing|noaudit]
Set the kernel audit condition to the *condition* specified where *condition* is the literal string **auditing** indicating auditing should be enabled or **noaudit** indicating auditing should be disabled.

-getclass *event* Display the preselection mask associated with the specified kernel audit event. *event* is the kernel event number or event name.

-setclass *event audit_flag*[*,audit_flag . . .*]
Map the kernel event *event* to the classes specified by *audit_flags*. *event* is an event number or name. An *audit_flag* is a two character string representing an audit class. See **audit_control**(4) for further information.

-lsevent Display the currently configured (runtime) kernel and user level audit event information.

-getpinfo *pid* Display the audit ID, preselection mask, terminal ID and audit session ID for the specified process.

-setpmask *pid flags*
Set the preselection mask of the specified process. **flags** is the ASCII representation of the flags similar to that in **audit_control**(4).

-setsmask *asid flags*
Set the preselection mask of all processes with the specified audit session ID.

-setumask *auid flags*
Set the preselection mask of all processes with the specified audit ID.

-lspolicy Display the kernel audit policies with a description of each policy.

-getpolicy Display the kernel audit policy.

-setpolicyf1[+ | -]*policy_flag*[,*policy_flag ...*]
Set the kernel audit policy. A policy *policy_flag* is literal strings that denotes an audit policy. A prefix of **+** adds the policies specified to the current audit policies. A prefix of **-** removes the policies specified from the current audit policies. The following are the valid policy flag strings (auditconfig -lspolicy also lists the current valid audit policy flag strings):

arge Include the **execv**(2) system call environment arguments to the audit record. This information is not included by default.

argv Include the **execv**(2) system call parameter arguments to the audit record. This information is not included by default.

cnt Do not suspend processes when audit resources are exhausted. Instead, drop audit records and keep a count of the number of records dropped. By default, process are suspended until audit resources become available.

group Include the supplementary group token in audit records. By default, the group token is not included.

path Add secondary path tokens to audit record. These are typically the pathnames of dynamically linked shared libraries or command interpreters for shell scripts. By default, they are not included.

trail Include the trailer token in every audit record. By default, the trailer token is not included.

seq Include the sequence token as part of every audit record. By default, the sequence token is not included. The sequence token attaches a sequence number to every audit record.

EXAMPLES

```
#
# map kernel audit event number 10 to the "fr" audit class
#
% auditconfig -setclass 10 fr

#
# turn on inclusion of exec arguments in exec audit records
#
% auditconfig -setpolicy +argv
```

ERRORS

auditconfig returns **0** upon success and **1** upon failure.

FILES

/etc/security/audit_event
/etc/security/audit_class

SEE ALSO

auditd(1M), **bsmconv**(1M), **praudit**(1M), **auditon**(2), **execv**(2), **audit_class**(4), **audit_control**(4), **audit_event**(4)