NAME

auditreduce - select records from audit trail files

SYNOPSIS

auditreduce [**-A**] [**-a** *YYYYMMDD*[*HH*[*MM*[*SS*]]]] [**-b** *YYYYMMDD*[*HH*[*MM*[*SS*]]]] [**-c** *flags*]
[**-d** *YYYYMMDD*] [**-e** *euid*] [**-f** *egid*] [**-g** *rgid*] [**-j** *id*] [**-m** *event*] [**-o** *object*=*value*] [**-r** *ruid*]
[**-u** *auid*] [**-v**] [**-z** *zone*] [*file ...*]

DESCRIPTION

The **auditreduce** utility selects records from the audit trail files based on the specified criteria. Matching audit records are printed to the standard output in their raw binary form. If no *file* argument is specified, the standard input is used by default. Use the praudit(1) utility to print the selected audit records in human-readable form.

The options are as follows:

-A Select all records.

-a *YYYYMMDD*[*HH*[*MM*[*SS*]]]
Select records that occurred after or on the given datetime.

-b *YYYYMMDD*[*HH*[*MM*[*SS*]]]
Select records that occurred before the given datetime.

-c *flags*
Select records matching the given audit classes specified as a comma separated list of audit flags. See audit_control(5) for a description of audit flags.

-d *YYYYMMDD*
Select records that occurred on a given date. This option cannot be used with **-a** or **-b**.

-e *euid*
Select records with the given effective user ID or name.

-f *egid*
Select records with the given effective group ID or name.

-g *rgid*
Select records with the given real group ID or name.

-j *id* Select records having a subject token with matching ID, where ID is a process ID.

-m *event*

Select records with the given event name or number. This option can be used more then once to select records of multiple event types. See audit_event(5) for a description of audit event names and numbers.

-o *object=value*

file Select records containing path tokens, where the pathname matches one of the comma delimited extended regular expression contained in given specification. Regular expressions which are prefixed with a tilde (‘~’) are excluded from the search results. These extended regular expressions are processed from left to right, and a path will either be selected or deslected based on the first match.

Since commas are used to delimit the regular expressions, a backslash (‘\’) character should be used to escape the comma if it is a part of the search pattern.

msgqid Select records containing the given message queue ID.

pid Select records containing the given process ID.

semid Select records containing the given semaphore ID.

shmid Select records containing the given shared memory ID.

-r *ruid*

Select records with the given real user ID or name.

-u *auid*

Select records with the given audit ID.

-v Invert sense of matching, to select records that do not match.

-z *zone*

Select records from the given zone(s). *zone* is a glob for zones to match.

EXAMPLES

To select all records associated with effective user ID root from the audit log */var/audit/20031016184719.20031017122634*:

```
auditreduce -e root \
    /var/audit/20031016184719.20031017122634
```

To select all setlogin(2) events from that log:

```
auditreduce -m AUE_SETLOGIN \
    /var/audit/20031016184719.20031017122634
```

Output from the above command lines will typically be piped to a new trail file, or via standard output to the praudit(1) command.

Select all records containing a path token where the pathname contains */etc/master.passwd*:

```
auditreduce -o file="/etc/master.passwd" \
    /var/audit/20031016184719.20031017122634
```

Select all records containing path tokens, where the pathname is a TTY device:

```
auditreduce -o file="/dev/tty[a-zA-Z][0-9]+" \
    /var/audit/20031016184719.20031017122634
```

Select all records containing path tokens, where the pathname is a TTY except for */dev/ttyp2*:

```
auditreduce -o file="~/dev/ttyp2,/dev/tty[a-zA-Z][0-9]+" \
    /var/audit/20031016184719.20031017122634
```

SEE ALSO

praudit(1), 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.