sun microsystems

Read This First

Software READ THIS FIRST Reference Manual Minibox

Sun Microsystems, Inc. • 2550 Garcia Avenue • Mountain View, CA 94043 • 415-960-1300

Part No: 800-1760-10
Revision A, of 9 May 1988

Read This First

Software READ THIS FIRST: Reference Manuals Minibox

Introduction

This document supplements the manuals contained in the Reference Manuals Minibox for Release 4.0 of the Sun Operating System (SunOS™).

Getting Help

If you discover problems with the material covered by enclosed Reference Manuals, call Sun Microsystems at: 1-800-USA-4SUN (1-800-872-4786). Have your system's model number and SunOS release number ready to give to the dispatcher.

You can also send questions by electronic mail to `sun!hotline`. Be sure to include your name, company, phone number, and SunOS release number in your mail message.

If you have questions about Sun's support services or your shipment, call your sales representative.

- To see the SunOS release number, type: **`cat /etc/motd`**

Documentation Errata and Additions

SunOS Reference Manual

Section 1

`make`(1)

The printed version of the `make`(1) page is formatted slightly differently than the on-line version. However, the technical content is identical.

`oldsetkeys`(1)

The on-line version of this page has SETKEYS in the page header. This is incorrect. The printed version correctly shows OLDSETKEYS in the page header.

sun microsystems

Revision A of 8 May 1988 Part No: 800-1760-10

unifdef(1)

The SYNOPSIS and OPTIONS sections incorrectly show options `-iu` and `-id`. These options should be shown as `-iU` and `-iD`, respectively.

Section 3

curses(3X)

The on-line version of this page omits the *Curses Functions* subheading.

getfaudflgs(3)

There should be a DIAGNOSTICS section noting that `-1` is returned on error and `0` on success.

getgraent(3)

There should be an ERRORS section noting that:

> Because read access is required on `/etc/security/group.adjunct`, `getgraent()` and `getgranam()` will fail unless the calling process has effective UID of root.

The files `/etc/security/group.adjunct` and `/var/yp/domainname/group.adjunct` should be mentioned in a FILES section.

getpwaent(3)

There should be an ERRORS section noting that:

> Because read access is required on `/etc/security/passwd.adjunct`, `getpwaent()` and *getpwanam()* will fail unless the calling process has effective UID of root.

The files `/etc/security/passwd.adjunct` and `/var/yp/`*domainname*`/passwd.adjunct.byname` should be mentioned in a FILES section.

random(3)

The on-line version of this page has a badly formatted example.

Section 5

Index Entries

A number of *Index* and *Global Index* entries for pages in Section 5 contain incorrect page-number references (first printing only).

resolv.conf(5)

The `/etc/resolv.conf` file is documented under the name `resolve.conf`(5) (a spurious "e" occurs after "`resolv`"). The FILES entry on this page incorrectly shows the file to be `/etc/resolve.conf`.

Section 8

Synopsis Errors

In the printed versions of the following pages, the indicated files are incorrectly shown to be in `/etc`; the on-line versions correctly show them to be in `/usr/etc`:

devnm(8)	**/usr**/etc/devnm
lockd(8C)	**/usr**/etc/rpc.lockd
routed(8C)	**/usr**/etc/in.routed
sendmail(8)	**/usr**/etc/sendmail
statd(8C)	**/usr**/etc/rpc.statd

audit_warn(8)

The SYNOPSIS should read:

`/usr/etc/audit_warn` [*option* [*arguments*]]

The first sentence of the DESCRIPTION should read:

The *audit_warn* script processes warning or error messages from the audit daemon. When a problem is encountered, the audit daemon, `auditd`(8) will call `audit_warn` with the appropriate option and arguments.

There should be an ENVIRONMENT section, noting the `RECIPIENTS` environment variable, as follows:

`RECIPIENTS`
defines who the system administrator(s) is (are) so that the error messages can be sent through electronic mail. The default user is root. The defined value(s) must contain valid mail addresses.

There should be an OPTIONS section as follows:

`soft` *file*
indicates that the soft limit for *file* has been exceeded. The default action for this option is to send mail to the system administrator.

`allsoft`
indicates that the soft limit for all filesystems has been exceeded. The default action for this option is to send mail to the system administrator.

`hard` *file*
indicates that the hard limit for file *file* has been exceeded. The default action for this option is to send mail to the system administrator.

`allhard` *count*
indicates that the hard limit for all filesystems has been exceeded *count* times. The default action for this option is to send mail to the system administrator only if the *count* is `1` and to send a message to the console every time. It is recommended that mail *not* be sent every time `audit_warn` is called with this option, since this might fill up another filesystem.

`ebusy`
indicates that the audit daemon is already running. The default action for this option is to send mail to the system administrator.

`tmpfile`
indicates that the temporary audit file already exists indicating a fatal error. The default action for this option is to send mail to the system administrator.

`nostart`
indicates that auditing cannot be started because the system audit state is `AUC_FCHDONE`. The default action for this option is to send mail to the system administrator. Some system administrators may prefer to have the script reboot the system at this point.

`auditoff`
indicates that someone other than the audit daemon changed the system audit state to something other than `AUC_AUDITING`. The audit daemon will have exited in this case. The default action for this option is to send mail to the system administrator.

`postsigterm`
indicates that an error occurred during the orderly shutdown of the audit daemon. The default action for this option is to send mail to the system administrator.

`getacdir`
indicates that there is a problem getting the directory list from `/etc/security/audit/audit_control`. The daemon will sleep until the file is fixed.

`auditd`(8)

The SYNOPSIS should read:

```
/usr/etc/auditd
```

The DESCRIPTION should read as follows:

The audit daemon controls the generation and location of audit trail files. If the function `issecure`(3) returns false, the only action that `auditd` takes is to disable the auditing system; otherwise, auditing is set up and started. If auditing is desired, `auditd` reads the `audit_control`(5) file to get a list of directories into which audit files can be written and the percentage limit for how much space to reserve on each filesystem before changing to the next directory.

If `auditd` receives the signal `SIGUSR1`, the current audit file is closed and another is opened. If `SIGHUP` is received, the current audit trail is closed, the `audit_control` file reread, and a new trail is opened. If `SIGTERM` is received the audit trail is closed and auditing is terminated. The program `audit`(8) sends these signals and is recommended for this purpose.

Each time the audit daemon opens a new audit trail file, it updates the file `audit_data`(5) to include the correct name.

There should be a DIAGNOSTICS section, as follows:

The audit daemon invokes the `audit_warn`(8) script under the following conditions.

`audit_warn soft` *pathname*

The file system upon which *pathname* resides has exceeded the minimum free space limit defined in `audit_control`(5). A new audit trail has been opened on another file system.

`audit_warn allsoft`

All available file systems have been filled beyond the minimum free space limit. A new audit trail has been opened anyway.

`audit_warn hard` *pathname*

The file system upon which *pathname* resides has filled or for some reason become unavailable. A new audit trail has been opened on another file system.

`audit_warn allhard` *count*

All available file systems have been filled or for some reason become unavailable. The audit daemon will repeat this call to `audit_warn` every twenty seconds until space becomes available. *count* is the number of times that audit_warn has been called since the problem arose.

`audit_warn ebusy`

There is already an audit daemon running.

`audit_warn tmpfile`

The file `/etc/security/audit/audit_tmp` exists, indicating a fatal error.

`audit_warn nostart`

The internal system audit condition is `AUC_FCHDONE`. Auditing cannot be started without rebooting the system.

`audit_warn auditoff`

The internal system audit condition has been changed to not be `AUC_AUDITING` by someone other than the audit daemon. This causes the audit daemon to exit.

`audit_warn postsigterm`

An error occurred during the orderly shutdown of the auditing system.

`audit_warn getacdir`

There is a problem getting the directory list from `/etc/security/audit/audit_control`. The audit daemon will hang in a sleep loop until this file is fixed.

`config`(8)

The printed SYNOPSIS incorrectly shows `config` as residing in `/etc`; it is in `/usr/etc`.

The path name to the "config" directory was changed from `/sys/conf` to `/usr/include/sys/conf`. This is incorrect. The correct path is `/usr/share/sys/`*arch*`/conf`. Because there is a symbolic link from `/sys`, the path `/sys/`*arch*`/conf` will also work.

`init`(8)

This page incorrectly implies that if the console is marked `secure` in `/etc/ttytab` then the system prompts for the root passowrd before coming up single-user. This is incorrect. The root password is required if the port is *not* marked `secure`.

`mount`(8)

The printed Reference Manual page, `mount`(8), should read as follows for the following `mount` options:

`ro` Mount the specified filesystem read-only, even if the entry in `/etc/fstab` specifies that it is to be mounted read-write.

`remount`
If the file system is currently mounted, and if the entry in `/etc/fstab` specifies that it is to be mounted read-write or `rw` was specified along with `remount`, remount the file system making it read-write. If the entry in `/etc/fstab` specifies that it is to be mounted read-only and `rw` was not specified, the file system is not remounted. If the file system is not currently mounted, an error results.

named(8)

The DESCRIPTION incorrectly refers to the daemon as `filenamed`. There is a SEE ALSO reference to `resolver`(5) which should refer to `resolv.conf`(5). As noted above, this page is (mistakenly) named `resolve.conf`(5).

praudit(8)

This page neglects to mention that no more than 100 audit files can be specified on the command line.