



© Copyright 2004 Hewlett-Packard Development Company, L.P.

Evaluated Configuration for Version 5.1A

This Best Practice contains the information necessary to configure the security features of the Tru64 UNIX Version 5.1A operating system to match the configuration used for the Common Criteria EAL1 certification. The evaluated release consists of Tru64 UNIX Version 5.1A configured as described in this Best Practice, combined with the evaluated release patch kit, `common_criteria_cert_kit_t64v51a`. The `common_criteria_cert_kit_t64v51a.tar` patch kit is available off of the [HP Support Web site](#) at

<http://www.itrc.hp.com/service/patch/mainPage.do>

You must register in order to use the support site. If you have not yet registered, do the following:

1. Click on the word “register”, on the above page
2. Fill out the requested registration information
3. Click on Next>>
4. Fill out the personal profile information
5. Click on Finish>>
6. Make sure you remember your User ID and Password.
7. Complete the registration process
8. Wait for registration to be activated

To get the patch kit off of the support web site do the following:

1. Enter your User ID and Password on the above page

2. Click on login>>
3. Under the heading "<> find individual patches" click on >> Tru64 UNIX
4. Select OS revision "5.1A/TCR5.1A"
5. Select Search by Keyword and "Common Criteria"
6. Click on Search>>
7. The search should find one match "COMMON_CRITERIA_CERT_T64V51A". Click on the box next to "COMMON_CRITERIA_CERT_T64V51A" in either the "Recommended" or "Most Recent" column.
8. Click on add to selected patch list>>
9. Click on download selected>>
10. In the "download items individually" section click on FTP>>
11. Use your browser to save the common_criteria_cert_t64v51a.tar file on your system

The common_criteria_cert_kit_t64v51a.tar patch kit is also available on the patch kit distribution CD-ROM as the common_criteria_cert_kit_t64v51a kit.

See the [Tru64 UNIX Best Practices Web page](#) for more information about other Best Practices documentation:

http://www.tru64unix.compaq.com/docs/best_practices

Is This Best Practice Right for You?

This configuration document is required by Common Criteria and might be of interest only to users who are required to replicate the environment under which the Common Criteria EAL1 certification was granted. To use this Best Practice, you must meet the requirements described in the following table:

Requirement	Description
Operating System	Tru64 UNIX Version 5.1A
Patch Designation	common_criteria_cert_kit_t64v51a
Hardware	AlphaServer platforms: 300, 400, 800, 1000, 1000A, 1200, 2000, 2100, 2100A, 4000, 4100, 8200, 8400, DS10, DS10L, DS20, DS20E, ES40, ES45, GS60E, GS80, GS140, GS160, and GS320. The following platforms are limited to single partition use: GS80, GS160, and GS320.
System Configuration	The system must be configured exactly as described in this document.
Access	The person performing the configuration needs root access to the

Requirement	Description
	system

Before You Begin

Before you apply the Best Practice for Evaluated Configuration, you must thoroughly understand UNIX security and the enhanced security features of the Tru64 UNIX operating system as documented in the Version 5.1A [Security](#) manual, including the implications of running in the Common Criteria EAL1 configuration. The *Security* manual is included on your documentation CD-ROM and is also available off of the [Tru64 UNIX documentation Web site](#):

<http://h30097.www3.hp.com/docs/>

To get to the Version 5.1A Security manual from the Tru64 UNIX documentation Web site: Click on “Tru64 UNIX Operating System”, then on “Tru64 UNIX Version 5.1A Online Documentation”, then on “System & Network Management Documentation Bookshelf”, then on either “HTML” or “PDF” next to “*Security*”.

You should also review the Version 5.1A installation procedures in the [Tru64 UNIX Version 5.1A Installation Guide](#), which is also included on your documentation CD-ROM and is also available on the [HP Tru64 UNIX Web site](#).

To get to the Version 5.1A *Installation Guide* from the Tru64 UNIX documentation Web site: Click on “Tru64 UNIX Operating System”, then on “Tru64 UNIX Version 5.1A Online Documentation”, then on “System & Network Management Documentation Bookshelf”, then on either “HTML” or “PDF” next to “*Installation Guide*”.

If you are not familiar with the HP patch process, see the [Tru64 UNIX patch Web site](#):

<http://www.support.compaq.com/patches>

and the [Patch Kit Installation Guide](#) on the [Tru64 UNIX patch documentation site](#):

<http://h30097.www3.hp.com/docs/patch>

To get to the Patch Kit Installation Guide from the Tru64 UNIX patch documentation site: Click on “HTML” or “PDF” next to “*Patch Kit Installation Instructions*”.

For the purposes of conforming to the EAL1 evaluated configuration, information in this Best Practice document supercedes any referenced document.

Applying the Best Practice

This procedure installs Tru64 UNIX Version 5.1A and the patch kit from CD_ROM. If your organization does not subscribe to HP's software update service, download the patch kit tar file from the Tru64 UNIX patch Web site, verify its integrity as instructed, and copy it to your own CD-ROM.

Until your system is fully configured, it should remain physically disconnected from any network.

The steps required to reproduce an evaluated configuration are the following:

- Installing the operating system
- Post-installation setup of authentication, auditing, and other security-related items
- Installing the patch kit
- Establishing customized parameters for system and network daemons.

Once configured, the system should be operated and maintained in accordance with the instructions, recommendations and guidance for secure operation as described in the *Tru64 UNIX Security* manual appendix E, C2 Level Security Configuration. Some of the procedures from that manual are additionally noted for your convenience in this document.

An evaluated configuration consists only of Tru64 UNIX Version 5.1A and the `common_criteria_cert_t64v51a` patch kit, installed on supported hardware, as described in this Best Practice. Including or deleting subsets, other than as described in this Best Practice, results in a configuration that does not conform to the EAL1 evaluated configuration. The addition of other patch kits or manually applied patches changes the evaluated configuration and invalidates the certification.

Installing the Operating System

To perform a full installation of Tru64 UNIX Version 5.1A on a single supported AlphaServer system, do the following:

1. From the console, boot the operating system CD-ROM using a command like the following:

```
>>> boot dqa0
```

2. Click OK for the English installation or select your preferred language.
3. Click Next to continue.
4. On the Host Information screen, enter the appropriate host name. The host name is the system name.
5. Enter the current date and time, the date is in US format (MM-DD-YYYY). Enter timezone and location information if necessary. Click Next to continue.
6. Enter a secure password for the root account. Click Next to continue.
7. From the Software Selection menu, select Customize. Click Next to continue.

8. From the Kernel Options menu, select Customize . Click Next to continue.
9. From the Select File System Layout menu, accept the Default File System Layout or configure the file system layout you require and continue by clicking Next.
10. Click Next again to go to the Installation Summary screen.
11. On the Installation Summary screen, click Edit List next to the Software Subsets: Customize option. The Software Subsets: Edit List screen is displayed.

Select the following optional subsets, in addition to the mandatory subsets:

- Reference Pages
 - Admin/User
- System Administration
 - Enhanced Security
 - Enhanced Security GUI
- Text Processing
 - Document Preparation Tools Extensions

Do not select or install any other optional subsets.

Note

When you accept the default file system layout (AdvFS) as the File System Type, the following subsets are installed as part of the mandatory subsets:

System
Administration—
AdvFS Commands
Kernel Build
Environment —
AdvFS Kernel
Modules

12. Click OK to continue.
13. On the Installation Summary screen, click Finish.
14. On the Ready to Begin Installation screen, click OK.

The installation continues and loads the software subsets onto the disk.

15. After the subsets load the system reboots. The Installation screen is then displayed from which you can select the kernel options. Select the Audit Subsystem option and confirm your selection. Do not select any other options.

16. When prompted to edit the configuration file, accept the default answer "n" by pressing the Enter key.

A new kernel is built and the system reboots with the new kernel.

Post Installation Security Related Setup

This section describes the post installation security related setup.

1. In the Login Window, enter the user name `root` and the password that you entered earlier. This action loads the Common Desktop Environment.
2. From the Tru64 UNIX System Setup menu, select Custom Setup.

The Checklist applications are used to configure the system, while the Checklist itself maintains a record of the configuration applications that have been completed. Use the Custom Setup Checklist.

3. On the Checklist, click License Manager.
4. On the License Manager, click Edit/New to enter your Tru64 UNIX license information on the New License screen. Click OK to save the entry.
5. On the Information screen, click OK to acknowledge that the entry has been registered and loaded.
6. Repeat steps 3 and 4 for each new license.
7. When you finish entering the licenses, click File/Exit .
8. If your system will be connected to a network, from the Checklist menu, choose Network Setup Wizard. Do the following:
 - a. Click Next to continue.
 - b. Configure your Network Interface Card as appropriate for your network configuration.
 - c. Click Next through the rest of the steps accepting the default configuration for each step.
 - d. Click Finish.
 - e. Do not connect your system to the network at this time.
9. From the Checklist menu, choose Security Configuration. Do the following:
 - a. Choose the ENHANCED system mode. Click Next to continue.
 - b. Click Next on the next two screens to advance to the System Options screen.
 - c. Click the check box next to Segment Sharing to disable segment sharing.
 - d. Click the check box next to Enable Access Control Lists to enable the access control lists. Click Next to continue.
 - e. When prompted, change the root password. Click Next to continue.
 - f. Click Next to skip the NIS option configuration.
 - g. Click Finish. Click OK to complete Security configuration.
10. From the Checklist menu, select the Audit Configuration Utility to enable security auditing as part of the system utilization. Do the following:
 - a. On the Welcome and Information screens, click Yes and click OK .

- b. Click Next to continue. This accepts the default destination for the audit data log.
 - c. On the Action On Log File Space Exhaustion screen, select Halt the system from the pull-down list of possible actions. Click Next to continue.
 - d. Click Next to continue and to accept the default lifespan for the audit log — forever.
 - e. On the Advanced Audit Options screen, click Finish part one.
 - f. On the Audit Event Information screen, click Yes to proceed to part two.
 - g. On the Audit Event Category Selection screen, select the timesharing-extended-audit and trusted event options. You can use Ctrl/click to select multiple options. Click Next.
 - h. Click Next to continue and to accept all defaults on the Advanced User Audit Event screen.
 - i. Click Next to continue and to accept the list of files subject to auditing.
 - j. On the Advanced options screen, deselect Include failed login user names if they don't exist in the password database. Click Finish.
 - k. On the Audit Configuration Complete screen ignore warnings for No such file or directory, click OK.
11. On the Custom Setup screen, click Exit.
 12. On the System Setup screen, click Exit.
 13. On the lower tool bar, click the up arrow (up-arrow) above the icon of the pencil and paper.
 14. Select Terminal to open a window on your system.
 15. Enter the following command to shut down your system:

```
# shutdown -h now
```

Installing the Patch Kit

This section explains how to install the patch kit.

1. Enter the following command to reboot the system to single-user mode to prepare for patch installation:

```
>>> boot -fl s
```

2. Enter the following command to prepare for patch installation:

```
# mount -a
```

3. From single-user mode, install the `common_criteria_cert_t64v51a` patch for Tru64 UNIX Version 5.1A as described in the patch kit documentation.

Note

While the patch kit documentation instructs you to always use the latest available kit, only the `common_criteria_cert_t64v51a` patch and Version 5.1A can be used for the evaluated configuration.

You can install the V5.1A patch kit from the CD-ROM or from a local directory.

4. Run the `dupatch` utility and answer the prompts as follows:

Top of patch distribution: patch directory on the CD-ROM or your local disk.

From the Main Menu, choose 1) Patch installation.

From the Patch Installation Menu, choose 2) Check and install patches in single user mode.

When prompted, `Do you want the patches to be reversible`, answer "n".

When prompted, `Your Name`, enter the name of the person doing the patch.

After you enter your name, you are prompted to enter any notes about the operation that you want stored for future reference. Enter a string similar to the following: "installation of the `common_criteria_cert_t64v51a` patch for the evaluated configuration". End your input with a period and press the Enter key.

Selecting patches: You are asked to enter your choices or to press Return to display the next screen. Press Return until the message, `Or you may choose one of the following options`, is displayed. Choose the option, `All of the above`.

The installation lists the patches. When prompted, `Is this correct`, enter "y".

Note that the patch kit contains patches for files in all subsets, including many not installed in this configuration. It is normal to see many of the following messages: `The patch will not be installed`.

Action to take: 1) Proceed with the n patches that passed the check.

When prompted, Do you have a pre-existing configuration file, enter "n".

When prompted, Enter a name for the kernel configuration file.
Accept the default.

When prompted, Do you want to replace it, enter "y".

When prompted to enter the Kernel options, select the Audit subsystem option.

When prompted, Do you want to edit the configuration file, enter "n".

Press Enter to page through the Special Instructions for patches installed.

The system displays the message Performing Kernel Build. After the kernel is built the message, A reboot is necessary to complete the patch installation, is displayed and you are prompted, Do you want to reboot the system now, enter "y".

The patch log is at `/var/adm/patch/log/session.log`.

Establishing Customized Security Parameters

After patch installation, reboot the system to multi-user mode and log in to the root account. To establish the appropriate security parameters required for secure operation of an evaluated configuration, do the following:

1. Set password control defaults for all user accounts.

By setting these values in the system default template, they will be applied to all users unless they are specifically overridden for an individual user.

Note that the maximum number of unsuccessful login attempts on the root account is set to 100. This is a tradeoff; a high value prevents a denial of service attack from locking out the root account. However, in an evaluated configuration, you should reset this value to five. The root account will always be allowed to log in to the physical console with the correct password.

```
# /usr/bin/X11/dxaccounts
```

- a. From the View menu, select Local Templates.
- b. Double-click the Default icon.
- c. Click Security.
- d. Under Turn To, select Password Controls.

- e. Specify a value of at least 8 for Minimum Chosen Length.
- f. Under Turn To, select Password Options. Verify how a clear (unset) and a set option box appear on your system for this screen. On some systems a box that is clear (unset) has light shading, a box that is set has dark shading. On other systems a box that is set has a white tick-mark. Some of the options may already be correctly clear or set.
- g. Clear the box marked Site Policy Generated.
- h. Clear the box marked System Generated.
- i. Clear the box marked Random Characters.
- j. Clear the box marked Random Letters.
- k. Set the box marked Triviality Checks.
- l. Under Turn To, select Login Restrictions.
- m. Set Maximum Attempts to 5.
- n. Click OK, then OK.
- o. From the View menu, select Local Users.
- p. Click the root icon.
- q. Click Security.
- r. Under Turn To, select Login Restrictions.
- s. Set Maximum Attempts to 5.
- t. Click OK, then OK.
- u. From the Options menu, select General. Verify how a clear (unset) and a set option box appear on your system for this screen. On some systems a box that is clear (unset) has light shading, a box that is set has dark shading. On other systems a box that is set has a white tick-mark. Some of the options may already be correctly clear or set.
- v. Clear the box marked Allow Duplicate User IDs.
- w. Clear the box marked Allow Duplicate Group IDs.
- x. Set the box marked Require Passwords for New Accounts.
- y. Click OK, and Accounts —> Close, to close `dxaccounts` and save the changes.

2. Verify and adjust the audit settings.

By following the steps of the Post Installation Security Related Setup section, you have already correctly configured most audit parameters. The settings ensure that the following conditions are established:

- o The audit subsystem does not lose audit data when disk space for the audit log file becomes full.
- o The audit log file is protected against access by unprivileged users.
- o The `/etc/sec/audit_events` file lists the correct set of events to be audited.

One additional audit parameter is required. The audit daemon should be configured to write its buffers to disk periodically in addition to writing when the buffers are full. This minimizes audit data loss in the event of hardware or power

failures. The interval selected for the buffer write is a business-management risk decision, trading potential loss of audit data against performance impact.

For example, to establish a 5-second interval, get the `AUDITD_FLAG` entry from `/etc/rc.config.common` and modify it to include `-d 5s`:

```
# /usr/sbin/rcmgr get AUDITD_FLAG
```

The above command returns the current `AUDITD_FLAG` value, for example:

```
-l /var/audit/auditlog -c syslog -o halt
```

Set the `AUDITD_FLAG` value, adding the `-d 5s` to the current value:

```
# /usr/sbin/rcmgr set AUDITD_FLAG -l \  
/var/audit/auditlog -c syslog -o halt -d 5s
```

3. Normally, a system booted to single-user mode is automatically logged in to the root account at the console. In an evaluated configuration, you must prohibit this behavior and force a password to be required in single-user mode with the following commands:

```
# /usr/sbin/rcmgr set SECURE_CONSOLE YES  
# /usr/sbin/rcmgr -n 0 set SECURITY ENHANCED
```

4. Set the defaults for the network and system daemons

Inbound network service requests are managed by the internet services daemon, `inetd`. `inetd`'s configuration file, `/etc/inetd.conf`, defines the network services that `inetd` will recognize.

Save a copy of the original `/etc/inetd.conf` file. Create a new `/etc/inetd.conf` file as outlined below. This restricts the inbound network service requests allowed by `inetd` to `telnet` and `ftp`.

```
# echo "telnet stream tcp nowait root /usr/sbin/telnetd telnetd" \  
>new_inetd
```

```
# echo "ftp stream tcp nowait root /usr/sbin/ftpd ftpd" >>new_inetd
```

```
# mv /etc/inetd.conf /saved_inetd.conf
```

```
# mv new_inetd /etc/inetd.conf
```

```
# chown bin:bin /etc/inetd.conf
```

```
# chmod 755 /etc/inetd.conf
```

5. Verify system parameters

Tru64 UNIX provides configurable settings that control system behavior. Most security-relevant tunables default to their most secure settings. This step describes how to verify that the settings are at their most secure and how to adjust settings, if necessary.

Consider the following `proc`, `vfs`, and `sec` subsystem settings:

- o `proc: executable_stack` should be set to 0
- o `proc: dump_cores` should be set to 0
- o `proc: dump_setugid_cores` should be set to 0
- o `sec: restricted_symlink_follow` should be set to 1
- o `sec: restricted_hardlink_creat` should be set to 1
- o `sec: restricted_fifo_open` should be set to 1
- o `vfs: follow_mkdir_symlinks` should be set to 0

To view and alter the `sysconfig` tunable settings:

```
# /usr/bin/X11/dxkerneltuner
```

Select the desired subsystem.

In the Boot Time column for each tunable, enter the correct value.

Click OK.

When all changes have been completed, under File, select Exit.

In Kernel Tuner Exit window click Keep the Changes.

6. Disable the system daemons

For ease of system administration, many system daemons are automatically started when the system boots. It is a good security rule to disable any daemon you do not use. The following daemons should always be disabled in an evaluated configuration:

- o Insight Manager

The `insightd` daemon provides remote system administration capabilities. Use the following command to prevent startup:

```
# /usr/sbin/rcmgr set INSIGHTD_CONF NO
```

- o `evm snmp trap handler daemon`

Use the following command to prevent startup:

```
# /usr/sbin/rcmgr set SNMPEVMD NO
```

- o smsd, snmpd, advfsd, and smauthd daemons

Remove the startup files from the system initialization path if they exist:

```
# mkdir /sbin/init.d/dont_start_these_daemons
```

```
# mv /sbin/init.d/smsd \  
/sbin/init.d/dont_start_these_daemons/
```

```
# mv /sbin/init.d/advfsd \  
/sbin/init.d/dont_start_these_daemons/
```

```
# mv /sbin/init.d/smauth \  
/sbin/init.d/dont_start_these_daemons/
```

```
# mv /sbin/init.d/snmpd \  
/sbin/init.d/dont_start_these_daemons/
```

- o lpd

Rename the lpd startup file:

```
# mv /sbin/init.d/lpd \  
/sbin/init.d/dont_start_these_daemons/
```

- o sendmail daemon

To disable the sendmail daemon from accepting inbound mail, use the following command:

```
# mv /sbin/init.d/sendmail \  
/sbin/init.d/dont_start_these_daemons
```

7. Prevent the syslog and binlog daemons from accepting remote connections.

To prevent the syslog and binlog daemons from accepting remote connections, use the following commands:

```
# touch /etc/syslog.auth
```

```
# touch /etc/binlog.auth
```

```
# chmod 600 /etc/syslog.auth
```

```
# chmod 600 /etc/binlog.auth
```

8. Restrict cron and at jobs to the root account only.

To explicitly restrict the creation of cron and at jobs to the root account only, use the following commands:

```
# echo "root" > /var/adm/cron/cron.allow
# echo "root" > /var/adm/cron/at.allow
# chmod 600 /var/adm/cron/cron.allow
# chmod 600 /var/adm/cron/at.allow
```

9. Configure the X Windowing System (XDM) as the graphical interface, rather than the Common Desktop Environment (CDE).

```
# /usr/sbin/rcmgr set XLOGIN xdm
```

10. Verify remote X Windows sessions are disabled.

Remote X Windows sessions are disabled by default. To verify this, use the command:

```
# /usr/bin/X11/xhost
```

If the xhost results show anything other than “access control enabled, only authorized clients can connect” use the command:

```
# /usr/bin/X11/xhost -
```

to disable all remote connections.

11. Enable object safety for all filesystems.

To enable object safety on each AdvFS Filesystem (only do this once, it persists across reboots):

```
# chfsets -o objectsafety domain_name fileset_name
```

To check that object safety is enabled on an AdvFS Filesystem:

```
# chfsets domain_name fileset_name
```

To enable object safety on all UFS Filesystems, create the file /etc/ufs_object_safety.stanza:

```
ufs:
```

```
ufs_object_safety = 1
```

Add the `ufs_object_safety` entry to the `/etc/sysconfigtab` file:

```
# sysconfigdb -a -f /etc/ufs_object_safety.stanza ufs
```

Object safety on UFS filesystems will not take effect until after the reboot in the following step..

To check that object safety is enabled on all UFS Filesystems:

```
# sysconfig -q ufs
```

12. Shut down the system, physically connect your system to the trusted network, and reboot the system to multi-user mode.

13. Install the `cchwtst` tool on your system.

- a. The `cchwtst` tool is available from the internet security software downloads site: <http://h30097.www3.hp.com/unix/security-download.html>. Select `cchwtst` from the additional security software list and download the kit.
- b. Use the `tar` command to expand the contents of the kit
- c. The file `README.txt` contains the instructions for installing the `cchwtst` tool on your system.

14. Verify the virtual memory protection mechanisms using the `cchwtst` tool.

This command tests a set of sample addresses for read and/or write access to verify the virtual memory protection. The command prints `SUCCESS` on success. If a failure occurs, the command displays information on the failing test and the status `FAILURE`.

```
#!/sbin/cchwtst
```

Procedures and Policies for Operating in the EAL1 Environment

This section discusses security policy considerations required to ensure secure operation. It also discusses the security implications of some operational changes you may choose to make. For more information, refer to the *Tru64 UNIX Security* manual, appendix E, C2 Level Security Configuration. HP recommends that you periodically review the items listed in Establishing Customized Security Parameters and verify that the current system settings are in compliance.

Using the Root Account

Any person with access to the root password must have the appropriate security clearance and be adequately trained for that role.

The root account must be used only in exceptional circumstances, as defined in your site security policy. Users empowered with root access must first log on using their own accounts and obtain root privileges using the `su` command. This procedure retains individual accountability for root actions.

Creating User Accounts

User account passwords must be at least eight characters in length, and triviality checks, to prevent easily guessable passwords, must be enabled. The maximum number of unsuccessful login attempts permitted before a user account is locked must be five.

Each user name must map to a unique user ID (UID) and each group name must map to a unique group ID (GID), to enforce individual accountability.

When creating a new user account, a system administrator must always enter an initial password using the password selection information in Section 2.4 of the V5.1A [Security](#) manual.

Changing a User's Password

The system administrator should not use the password button on the `dxaccounts` window to change a user's password. The system administrator should double click on the user in the `dxaccounts` window and use the Password... button or use the `/usr/bin/passwd` command from the command line if it is necessary to change a user's password.

Using the System Console

Any person with access to the system console must have the appropriate security clearance and be adequately trained for that role. The system console must reside in a physically secured area that is only accessible by the system administrators..

Installing Software

Before installing an application using the `setld` utility, always shut the system down to single-user mode and remove files from the `/tmp`, `/usr/tmp`, and `/var/tmp` directories with the `/usr/sbin/dirclean` utility.

Preserving the Audit Logs

If you must remove audit logs from the system to prevent the audit log overflow condition or for any other reason, the audit logs should be copied to secure removable media and stored in a secure location.

Recovering Audit Data After a System Crash

After a system crash, restart the system in single-user mode. Check to see if the audit logs have overflowed the audit log overflow threshold (the filesystem is more than 90 percent full). If necessary, free space on the filesystem before bringing the system to multiuser mode.

The audit data in memory at the time of the crash is automatically recovered and stored in `/var/adm/crash/audit-data.{crash number}`. To view this data, copy the file to `/var/audit`, rename it `auditlog.{system}.{next_in_sequence}`, and view with `/usr/sbin/audit_tool`. If there was no audit data present in memory at the time of the crash, the data file will not be created.

Changing the System Time

Every audit event is recorded with a timestamp. Check the system time weekly. If the system time has changed so that it is not sufficiently accurate for you to evaluate the information in the audit logs, update the system time as follows:

1. Shutdown the system to single-user mode.
2. Use the `date (1)` command to change the system time.
3. If you have changed the time such that when you return the system to multiuser mode the audit logs will contain events that overlap existing events, you will have to move the current set of audit log files from the audit directory in order to preserve the sequence of events.
4. Return the system to multi-user mode.

Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

best_practices@zk3.dec.com

Legal Notice

UNIX® and The Open Group™ are trademarks of The Open Group™ in the U.S. and/or other countries. All other product names mentioned herein may be trademarks of their respective companies.

Confidential computer software. Valid license from HP and/or its subsidiaries required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Neither HP nor any of its subsidiaries shall be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.
