Tru64 UNIX 4.0F and TruCluster 1.6

Patch Summary and Release Notes for Patch Kit-0004

June 2000

This manual describes the release notes and contents of Patch Kit-0004. It provides any special instructions for installing individual patches.

For information about installing or removing patches, baselining, and general patch management, see the *Patch Kit Installation Instructions*.

Compaq Computer Corporation
Houston, Texas

Contents

About This Manual

This manual contains information specific to Patch Kit-0004 for the Tru64TM™ UNIX Version 4.0F operating system and TruClusterTM™ 1.6 software product. It provides a list of the patches contained in each kit and describes any information you need to know when installing specific patches.

For information about installing or removing patches, baselining, and general patch management, see the *Patch Kit Installation Instructions*.

Audience

This manual is for the person who installs and removes the patch kit and for anyone who manages patches after they are installed.

Organization

This manual is organized as follows:

Chapter 1 Contains the release notes for this patch kit.

Chapter 2 Summarizes the base operating system patches included in the kit.

Chapter 3 Summarizes the TruCluster software patches included in the kit.

Related Documentation

In addition to this manual, you should be familiar with the concepts and mechanisms described in the following Tru64 UNIX and TruCluster (TCR) documents:

- Tru64 UNIX and TCR *Patch Kit Installation Instructions*
- Tru64 UNIX *Installation Guide*
- Tru64 UNIX *System Administration*
- TruCluster Software Products *Software Installation*
- TruCluster Software Products *Cluster Administration*
- Any release-specific installation documentation

Reader's Comments

Compaq welcomes any comments and suggestions you have on this and other Tru64 UNIX manuals.

You can send your comments in the following ways:

- Fax: 603-884-0120 Attn: UBPG Publications, ZK03-3/Y32
- Internet electronic mail: `readers_comment@zk3.dec.com`

  A Reader's Comment form is located on your system in the following location:

  `/usr/doc/readers_comment.txt`

- Mail:

  Compaq Computer Corporation
  UBPG Publications Manager
  ZK03-3/Y32
  110 Spit Brook Road
  Nashua, NH 03062-9987

Please include the following information along with your comments:

- The full title of this document.
- The section numbers and page numbers of the information on which you are commenting.
- The version of Tru64 UNIX that you are using.
- The version of TruCluster software that you are using.
- If known, the type of processor that is running the Tru64 UNIX software.

The Tru64 UNIX Publications group cannot respond to system problems or technical support inquiries. Please address technical questions to your local system vendor or to the appropriate Compaq technical support office. Information provided with the software media explains how to send problem reports to Compaq.

1

Release Notes

This chapter provides information that you must be aware of when working with Tru64 UNIX 4.0F and TCR 1.6 Patch Kit-0004.

1.1 Required Storage Space

The following storage space is required to successfully install this patch kit:

Base Operating System

- Temporary Storage Space

  A total of ~250 MB of storage space is required to untar this patch kit. It is recommended that this kit not be placed in the /, /usr, or /var file systems because this may unduly constrain the available storage space for the patching activity.

- Permanent Storage Space

  Up to ~42.6 MB of storage space in /var/adm/patch/backup may be required for archived original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~403 MB of storage space in /var/adm/patch may be required for original files if you choose to install and revert all patches. See *Patch Kit Installation Instructions* for more information.

  Up to ~515 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~136 KB of storage space is needed in /usr/sbin/dupatch for the patch management utility.

TruCluster Software Products

- Temporary Storage Space

  A total of ~250 MB of storage space is required to untar this patch kit. It is recommended that this kit not be placed in the /, /usr, or /var file systems because this may unduly constrain the available storage space for the patching activity.

- Permanent Storage Space

  Up to ~59.6 MB of storage space in /var/adm/patch/backup may be required for archived original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~60 MB of storage space in /var/adm/patch may be required for original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~649 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~136 KB of storage space is needed in /usr/sbin/dupatch for the patch management utility.

1.2 New dupatch Features

Beginning with Revision 26–02 of `dupatch`, this patch tool utility has been enhanced to provide new features, as described in the following sections. For more information, see the *Patch Kit Installation Instructions*.

1.2.1 Patch Installation from Multiuser Mode

Patches can now be installed when a system is in multiuser mode.

There are no restrictions on performing patch selection and preinstallation checking in multiuser mode.

However, although you can now install patches in multiuser mode, Compaq recommends that you bring down your system to single-user mode when installing patches that affect the operation of the Tru64 UNIX operating system (or the product you are patching). If your system must remain in multiuser mode, it is recommended that you apply the patches when the system is as lightly loaded as possible.

1.2.2 Automatic Kernel Build

If the patches installed indicate that a kernel build is required, `dupatch` will initiate the kernel build automatically.

Most times a reboot is required to complete the installation and bring the system to a consistent running environment. Certain file types, such as libraries, are not moved into place until you reboot the system.

When installing patches in multiuser mode, you can take one of three options after the kernel build is complete:

- Reboot the system immediately.
- Reboot the system at a specified time.
- Forgo a system reboot.

1.2.3 Patch Installation from a Pseudo-Terminal

Patches can now be installed on the system from a pseudo-terminal (pty) while in single-user mode. To do this, log into the system as root from a remote location and specify that the patches are to be installed in single-user mode. Once all the patch prerequisites are completed, the system will be taken to single-user mode while maintaining the network connection for the root user. The patches will then be installed by the system.

1.3 Release Notes for Patch 342.00

This release notes contains the new reference page for `ttauth`.

NAME

ttauth - ToolTalk authority file utility

SYNOPSIS

ttauth [[-f] | [authfile]] [[-vqib]] [[command arg ...]]

DESCRIPTION

The ttauth program is used to edit and display the authorization information used in connecting to ToolTalk. This program is usually used to extract authorization records from one machine and merge them in on another (as is the case when using remote logins or granting access to

other users). Commands (described below) may be entered interactively, on the ttauth command line, or in scripts. Note that this program does not contact the ToolTalk server, ttsession. Normally ttauth is not used to create the authority file entry in the first place; ttsession does that.

OPTIONS

The following options may be used with ttauth. They may be given individually or may combined.

-f authfile
This option specifies the name of the authority file to use. By default, ttauth uses the file specified by the TTAUTHORITY environment variable or the .TTauthority file in the user's home directory.

-q This option indicates that ttauth should operate quietly and not print unsolicited status messages. This is the default if an ttauth command is given on the command line or if the standard output is not directed to a terminal.

-v This option indicates that ttauth should operate verbosely and print status messages indicating the results of various operations (for example, how many records have been read in or written out). This is the default if ttauth is reading commands from its standard input and its standard output is directed to a terminal.

-i This option indicates that ttauth should ignore any authority file locks. Normally, ttauth refuses to read or edit any authority files that have been locked by other programs (usually ttsession or another ttauth).

-b This option indicates that ttauth should attempt to break any authority file locks before proceeding. Use this option only to clean up stale locks.

COMMANDS

The following commands may be used to manipulate authority files:

add protoname protodata netid authname authdata
An authorization entry for the indicated ToolTalk session using the given protocol name (protoname), protocol data (protodata), ToolTalk session id (netid), authentication name (authname), and authentication data (authdata) is added to the authorization file. The protocol name should always be the string "TT". The protocol data should always be the empty string. The ToolTalk session ID is formatted string consisting of the ttsession program number, the ttsession authorization level, the IP address of the host running ttsession, and the RPC version number of the ttsession. See the TTSESSION IDENTIFIERS section below for information on constructing ToolTalk session ID's for the authority file. The authentication name should always be the string "MIT-MAGIC-COOKIE-1". The authentication data is specified as an even-lengthed string of hexadecimal digits, each pair representing one octet. The first digit of each pair gives the most significant 4 bits of the octet, and the second digit of the pair gives the least significant 4 bits. For example, a 32 character hexkey would represent a 128-bit value.

[n]extract filename Authorization entries which match the specified fields are written to the indicated file. If the nextract command is used, the entries are written in a numeric format suitable for non-binary transmission (such as secure electronic mail). The extracted entries can be read back in using the merge and nmerge commands. If the file name consists of just a single dash, the entries will be written to the standard output.

[n]list Authorization entries which match the specified fields (or all if nothing is specified) are printed on the standard output.

If the nlist command is used, entries are shown in the numeric format used by the nextract command; otherwise, they are shown in a textual format. Key data is always displayed in the hexadecimal format given in the description of the add command.

[n]merge [filename1 ...]
Authorization entries are read from the specified files and are merged into the authorization database, superseding any matching existing entries. If the nmerge command is used, the numeric format given in the description of the extract command is used. If a file name consists of just a single dash, the standard input will be read if it hasn't been read before.

remove Authorization entries which match the specified fields are removed from the authority file.

source filename
The specified file is treated as a script containing ttauth commands to execute. Blank lines and lines beginning with a pound sign (#) are ignored. A single dash may be used to indicate the standard input, if it has not already been read.

info Information describing the authorization file, whether or not any changes have been made, and from where ttauth commands are being read is printed on the standard output.

exit If any modifications have been made, the authority file is written out (if allowed), and the program exits. An end of file is treated as an implicit exit command.

quit The program exits, ignoring any modifications. This may also be accomplished by pressing the interrupt character.

help [string]
A description of all commands that begin with the given string (or all commands if no string is given) is printed on the standard output.

? A short list of the valid commands is printed on the standard output.

TTSESSION IDENTIFIERS

The ToolTalk session identifiers (netid) in the authority file and used by the add, [n]extract, [n]list, and remove commands are derived from the TT_SESSION identifier constructed by ttsession at startup. The ttsession rendezvous with clients by writing the TT_SESSION identifier as a property on the root window or as an environment variable in the client's environment (see ttsession -c). In addition, ttsession creates an entry in the user's authority file. The authority file entry has a netid component which is derived from the TT_SESSION identifier.

The TT_SESSION(STRING) = "01 1433 1342177279 1 1 2002 130.105.9.22 4" identifier is composed of the following elements:

```
 <Dummy Number>                 = 01
 <ttsession Process Id>         = 1433
<ttsession Program Number>      = 1342177279
<DummyNumber>                   = 1
<ttsession Authorization Level> = 1
<ttsession UID>                 = 2002
<Host IP Address>               = 130.105.9.22
<RPC Version Number>            = 4
```

The ToolTalk session identifiers (netid) in the authority file are composed of the <ttsession Program Number>, <ttsession Authorization Level>, <Host IP Address>, and <RPC Version Number> fields of the TT_SESSION identifier as follows:

1342177279/1/130.105.9.22/4

EXAMPLE

The most common use for ttauth is to extract the entry for the current ttsession, copy it to another machine, and merge it into the user's authority file on the remote machine:

```
% xprop -root | grep TT_SESSION

TT_SESSION(STRING) = "01 1433 1342177279 1 1 2002 130.105.9.22 4"
_SUN_TT_SESSION(STRING) = "01 1433 1342177279 1 1 2002 130.105.9.22 4"

% ttauth extract - netid=1342177279/1/130.105.9.22/4 | rsh otherhost ttauth
merge -
```

ENVIRONMENT

This ttauth program uses the following environment variables:

TTAUTHORITY
Gets the name of the authority file to use if the -f option is not used.

FILES

.TTauthority
Default authority file in the user's home directory if TTAUTHORITY is not defined.

RESTRICTIONS

Users that have unsecure networks should take care to use encrypted file transfer mechanisms to copy authorization entries between machines. Similarly, the MIT-MAGIC-COOKIE-1 protocol is not very useful in unsecure environments. Sites that are interested in additional security may need to use encrypted authorization mechanisms such as Kerberos.

Spaces are currently not allowed in the protocol name. Quoting could be added for the truly perverse.

SEE ALSO

Commands: ttsession(1)

ToolTalk Reference Manual

The options section of the ttsession manpage should now look like this:

-a level
Set the server authentication level. The following level string values are supported:

cookie
The sender and receiver must share the same cookie. This means that messages which do not specify a handler "ptype" are delivered even if the cookies do not match. This is the default authorization scheme. For "full security" use the -F option. Refer to the ttauth(1) reference page for more information.

1.4 Release Notes for Patch 456.00

This section contains release notes for Patch 456.00.

1.4.1 UFS Delayed Metadata mount Option

This new `mount` option allows for disabling synchronous metadata writes on a specified filesystem. The new `mount` option name is `delayed`.

To maintain the file system's consistency, UFS metadata (such as inode, directory, and indirect blocks) is updated synchronously by default.

Metadata updates are typically performed synchronously to prevent filesystem corruption after a crash. The trade-off for this filesystem integrity, however, is performance. In some cases, such as a filesystem serving as a cache, performance (faster metadata update) is more important than preserving data consistency across a system crash; for example, files under `/tmp` or web proxy servers such as Squid.

This means two things. One is that multiple updates to one block becomes only one block write, as opposed to multiple writes of the same block with traditional synchronous metadata update. The other is that users can experience much better responsiveness when they run metadata intensive applications because metadata writes will not go out to the disk immediately while users get their prompt back as soon as the metadata updates are queued.

This `delayed` option should not be used on the `/` or `/usr` filesystems. It should be used only on filesystems that do not need to survive across a system crash.

To enable the `delayed` option, run:

```
mount -o delayed
```

or

```
mount -u -o delayed mount -u -o delayed
```

1.4.2 PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA)

This patch provides the driver support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA) (also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB). To obtain full support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA), you must also select Patch 359.00, which is the X server portion of the patch.

1.4.3 Intelligent I/O Disks with mnemonic ri

If Patch 456.00 is installed on a system with Intelligent I/O (I2O) disks that use the device identifier, `mnemonic ri`, Patch 187.00 should also be installed if the user uses the `diskconfig` utility. Without Patch 187.00, the `diskconfig` utility will not recognize or configure the Intelligent I/O (I2O) disks.

1.4.4 Virtual Memory Problem

Installing Patch 456.00 on a system running Tru64 UNIX 4.0D through 4.0F may cause the system to crash if you run an application that maps a large number of file system objects into virtual memory using the `mmap`(2) function call. This problem may occur with large threaded applications, such as the Netscape Enterprise Web Server, which use this technique to improve performance and scalibility.

To avoid this problem, disable the kernel's virtual memory (`vm:`) subsystem attribute `vm-map-index-enable` after installing the patch and before rebooting the system. The attribute is disabled when its value is set to zero at boot time.

Enter the following commands at the shell prompt (when logged in as root) to add or modify the `vm-map-index-enable` attribute entry in the `/etc/sysconfigtab` file:

```
$ su root
$ cat << _EOF_ > /tmp/vm.stanza
> vm:
> vm-map-index-enabled=0
> _EOF_
$ sysconfigdb -m -f /tmp/vm.stanza vm
$rm -f /tmp/vm.stanza
$ reboot
```

See the sysconfigdb(8) man page for additional information.

This problem will be fixed in the next release of the patch kits.

1.4.5 PCI To Ethernet/Graphics Combo Adapter

This patch provides support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA). If you have a system with this adapter, you will need to reconfigure and rebuild the kernel after installing this patch. To do this:

1. Shut down the system:

   # **/usr/sbin/shutdown -h now**

2. Boot genvmunix to single-user mode:

   >>> **boot -fi genvmunix -fl s**

3. After the system boots to single-user mode, mount the file systems, run the update command, and activate the swap partition:

   # **/sbin/bcheckrc**

   # **/sbin/update**

   # **/sbin/swapon -a**

4. Run doconfig to create a new kernel configuration file and rebuild the kernel:

   # **/usr/sbin/doconfig**

   Note

   Do not specify the -c option to doconfig. If you do, doconfig will use the existing kernel configuration file, which will not have the appropriate controller entry for the PCI To Ethernet/Graphics Combo Adapter.

5. Save the old /vmunix file and move the new kernel to /vmunix.

6. Shut down the system:

   # **/usr/sbin/shutdown -h now**

7. Boot the new kernel:

   >>> **boot**

If you remove this patch from your system after you have rebuilt the kernel, to incorporate support for the PCI To Ethernet/Graphics Combo Adapter as previously described, you will need to rebuild the kernel again to restore generic VGA graphics support. To do this, follow the steps previously given.

If doconfig is running on the original kernel, the unpatched genvmunix will not recognize the PCI To Ethernet/Graphics Combo Adapter and will include generic VGA graphics support in the resulting kernel.

1.4.6 Pleiades II Switches

To determine if target IDs are being consumed by the switch, look at the contents of the /etc/emx.info file. If a FC Port Name exists that does not start with 0x0050 (a HSG80) or a 0x0010 (a KGPSA), it is most likely a switch entry consuming the target ID (or an unsupported FC device exists on the fabric).

To remove the switch entry from the emx target ID mappings, in addition to installing this patch, the /sys/data/emx_data.c file must be modified to contain the switch entry to be deleted (by setting the target ID to -1). See the reference pages for emx and emx_data.c for instructions on modifying the emx_data.c file.

After the emx_data.c file has been modified, the kernel must be regenerated and the resulting kernel booted.

1.4.7 I/O Throttling/Smooth Sync

Note

Smooth Sync is for UNIX File System (UFS) only.

Note

To activate I/O Throttling/Smooth Sync, you must install Patch 299.00.

The new mount options are smsync2 and throttle. The smsync2 option enables an alternate smsync policy in which dirty pages do not get flushed until they have been dirty and idle for the smoothsync age period (the default 30 is seconds). The default policy is to flush dirty pages after being dirty for the smoothsync age period, regardless of continued modifications to the page. Note that mmaped pages always use this default policy, regardless of the smsync2 setting.

For example, change the /etc/fstab entries from:

```
/dev/rz12e /mnt/test ufs rw 0 2
```

to:

```
/dev/rz12e /mnt/test ufs rw,smsync2,throttle 0 2
```

Note

If you choose not to use smsync2 (which does not affect mmaped buffers), just remove the smsync2 option from the previous string.

Append any tuning changes to /etc/sysconfigtab. See the TUNING notes that follow for a description of the new io-throttle-shift and io-throttle-maxmzthruput tunables. These tunables are configured in the vfs stanza. The following three lines make up an example:

```
vfs:

io-throttle-shift = 1

io-throttle-maxmzthruput = 1
```

When removing this patch, follow these steps:

1. Remove the lines added above to /etc/inittab.
2. Remove any additions to /etc/fstab you may have made (see previous instructions).

Failure to remove /etc/inittab and /etc/fstab modifications may result in unknown attribute messages, particularly upon system reboot.

TUNING

The purpose of this patch is to minimize system stalls resulting from a heavy system I/O load. This patch introduces a smoothsync approach to writing delayed I/O requests and introduces I/O throttling.

Using smoothsync allows each dirty page to age for a specified time period before getting pushed to disk. This allows more opportunity for frequently modified pages

to be found in the cache, which decreases the net I/O load. Also, as pages are enqueued to a device after having aged sufficiently, as opposed to getting flushed by the update daemon, spikes are minimized in which large numbers of dirty pages are locked on the device queue.

I/O throttling further addresses the concern of locking dirty pages on the device queue. It enforces a limit on the number of delayed I/O requests allowed to be on the device queue at any point in time. This allows the system to be more responsive to any synchronous requests added to the device queue, such as a read or the loading of a new program into memory. This may decrease the duration of process stalls for specific dirty buffers, as pages remain available until placed on the device queue.

The relevant tunable variables are:

`smoothsync-age`

This variable can be adjusted from 0 (off) up to 300. This is the number of seconds a page ages before becoming eligible for being flushed to disk via the smoothsync mechanism. A value of 30 corresponds to the "guarantee" provided by the traditional UNIX update mechanism. Increasing this value increases the exposure of lost data should the system crash, but can decrease net I/O load (to improve performance) by allowing the dirty data to remain in cache longer. In some environments, any data that is not up to date is useless; these are prime candidates for an increased `smoothsync-age` value. The default value of `smoothsync-age` is 30.

`io-throttle-shift`

The greater the number of requests on an I/O device queue, the longer the time required to process those requests and make those pages and device available. The number of concurrent delayed I/O requests on an I/O device queue can be throttled by setting the `io-throttle-shift` tunable. The throttle value is based on this tunable and the calculated I/O completion rate. The throttle value is proportional to the time required to process the I/O device queue. The correspondences between `io-throttle-shift` values and the time to process the device queue are:

io-throttle-shift	time to process device queue (sec)
-2	0.25
-1	0.5
0	1
1	2
2	4

For example, an `io-throttle-shift` value of 0 corresponds to accommodating 1 second of I/O requests. The valid range for this tunable is [-4..4] (not all values are shown in the previous table; you can extrapolate). The default value of `io-throttle-shift` is 1. Environments particularly sensitive to delays in accessing the I/O device might consider reducing the `io-throttle-shift` value.

`io-maxmzthruput`

This is a toggle that trades off maximizing I/O throughput against maximizing the availability of dirty pages. Maximizing I/O throughput works more aggressively to keep the device busy, but within the constraints of the throttle. Maximizing the availability of dirty pages is more aggressive at decreasing stall time experienced when waiting for dirty pages.

The environment in which you might consider setting `io-maxmzthruput off` (0) is one in which I/O is confined to a small number of I/O–intensive applications, such that access to a specific set of pages becomes more important for overall performance than does keeping the I/O device busy. The default value of `io-maxmzthruput` is 1. Environments particularly sensitive to delays in accessing sets of frequently used dirty pages might consider setting `io-maxmzthruput` to 0.

1.4.8 Granularity Hint Regions Restriction Removal

This patch removes a Granularity Hint Regions (also called GH chunks) restriction which may be encountered on AlphaServerTM™ DS20 and ES40 systems running the Tru64 UNIX Version 4.0F release. This restriction can reduce performance for certain database applications.

The following error message on the system's console terminal (also logged in `/var/adm/messages`) indicates possible performance loss for applications using GH chunks:

```
gh_chunks value of # invalid
```

where # is a number that varies depending on memory size.

To remove the GH chunks restriction, you need to modify your target kernel configuration file (and rebuild the kernel) and change the state of a console firmware environment variable. To make these changes, follow these steps:

1. Follow the steps in Section 4.5.3 of the *Guide to System Adminstration*, with the following exceptions:

   In step 4, edit the configuration file and add the following line immediately before the first line starting with `makeoptions`:

   ```
   makeoptions LOADADDR="fffffc0000430000"
   ```

   In step 6, instead of `/usr/sbin/shutdown -r now`, add the following line:

   ```
   /usr/sbin/shutdown -h now
   ```

2. Check the console firmware version:

   ```
   P00>>>show version
   ```

   If the version is not V5.5 or later, you need to upgrade your firmware to V5.5 or later.

3. Change the value of the `console_memory_allocation` environment variable from `old` to `new` and reset the system:

   ```
   P00>>>set console_memory_allocation new
   P00>>>init
   ```

4. Boot the new kernel:

   ```
   P00>>>boot
   ```

   If the new kernel fails to boot use one of the following procedures:

   ```
   P00>>>set console_memory_allocation old
   P00>>>init
   P00>>>boot -fi vmunix.save
   ```

   or:

   ```
   P00>>>boot -fi genvmunix
   ```

   Correct the error and repeat the previous procedure.

Additional Information

- If you encounter the following error message, you have most likely attempted to boot a kernel with the old load address:

  ```
  Bootstrap address collision, image loading aborted
  ```

  To boot old kernels:

  ```
  P00>>>set console_memory_allocation old
  P00>>>init
  ```

```
P00>>>boot
```

Note

The generic kernel (/genvmunix) will boot with console_memory_allocation set to old or new.

- The patch kit installs a new /usr/sbin/sizer command. If you rebuild the kernel using Section 4.5.1 or 4.5.2 of the *System Administration Manual*, the new sizer will automatically adjust the kernel's load address.

Note

If you customized your existing configuration file, doconfig allows you to edit the new configuration file so you can restore your customizations.

1.5 Release Notes for Patch 457.00

The following release notes provide Visual Threads Upgrade information and updated information for the quotacheck(8), fsck(8), and fstab(4) reference pages.

1.5.1 Visual Threads Upgrade Required

Visual Threads users will need to upgrade to the latest version of Visual Threads for the race detection rules to work. The Visual Threads upgrade is available from http://www.tru64unix.compaq.com/visualthreads and will be available in the next Developers' Tooklit Supplement.

1.5.2 quotacheck(8), fsck(8), and fstab(4) Reference Pages

quotacheck(8) Reference Page Update

SYNOPSIS

/usr/sbin/quotacheck [-guv] filesystem ...

OLD> /usr/sbin/quotacheck -a [-guv] [-l number]
NEW> /usr/sbin/quotacheck -a [-guv] [-l number] [-t [no]type]

FLAGS

OLD> -a Checks all file systems identified in the /etc/fstab file as read/write with disk quotas.

NEW> -a Checks all UFS and AdvFS file systems identified in the /etc/fstab file as read/write with userquota and/or groupquota options specified, and a pass number of 1 or greater. If the -t option is specified, only the file systems of the specified type will be checked. Alternatively, if type is prefixed with 'no', then the valid file systems in the /etc/fstab file that do not have that type will be checked.

OLD> -l number Specifies the number of times to perform disk quota checking.

NEW> -l number Specifies the maximum number of parallel quotacheck processes to run at one time.

NEW> -t [no]type
NEW> Specifies the file system type. The supported file systems are

as follows:

advfs - Advanced File System (AdvFS)

ufs - UNIX File System (UFS)

See fstab(4) for a description of file system types. If the 'no' prefix is used, all of the above file types except the one specified are checked.

Note, the -t flag is only valid when used with the -a flag.

DESCRIPTION

OLD> The quotacheck command examines each specified file system, builds a table of current disk usage, and compares this table against that stored in the disk quota file for the file system. If any inconsistencies are detected, both the quota file and the current system copy of the incorrect quotas are updated. Each file system must be mounted with quotas enabled.

NEW> The quotacheck command examines each specified file system, builds a table of current disk usage, and compares this table against that stored in the disk quota file for the file system. If any inconsistencies are detected, both the quota file and the current system copy of the incorrect quotas are updated.

OLD> The quotacheck command runs parallel passes on file systems using the number specified in the fsck field of the file system's entry in the /etc/fstab file. The quotacheck command only checks file systems with pass number 1 or higher in the fsck field. A file system with no pass number is not checked.

NEW> The quotacheck -a command runs parallel passes on file systems using the number specified in the /etc/fstab pass number field. The quotacheck command only checks file systems with pass number 1 or higher in the fsck field. A file system with no pass number is not checked.

OLD> For both UFS file systems and AdvFS filesets, you should assign the root file system a fsck field value of 1, and a value of 2 or higher to other file systems. See fstab(4) for more information.

NEW> For both UFS file systems and AdvFS filesets, you should assign the root file system a pass number of 1, and a value of 2 or higher to other file systems. See fstab(4) for more information.

OLD> The quotacheck command checks only file systems that have the userquota or groupquota option specified in the /etc/fstab file.

NEW> The quotacheck command checks only file systems that are mounted. UFS file systems must also have userquota and/or groupquota options specified in the /etc/fstab file. The userquota and groupquota options are only needed for AdvFS file systems if quotas are actually going to be enforced or if they are to be selected with the -a option.

fsck(8) Reference Page Update

OLD> When the system boots, the fsck program is automatically run with the -p flag. The program reads the /etc/fstab file to determine which file systems to check. Only partitions that are specified in the fstab file as being mounted “rw” or “ro” and that have a non-zero pass number are checked. File systems that have a pass number 1 (usually only the root file system) are checked one at a time. When pass 1 completes, all the remaining file systems are checked, with one process running per disk drive.

NEW> When the system boots, the fsck program is automatically run with the -p flag. The program reads the /etc/fstab file to determine which file systems to check. Only partitions that

are specified in the fstab file as being mounted “rw” or “ro” and that have a non-zero pass number are checked. File systems that have a pass number 1 (usually only the root file system) are checked one at a time. When pass 1 completes, the remaining pass numbers are processed with one parallel fsck process running per disk drive in the same pass.

NEW> The per disk drive logic is based on the /dev/disk/dsk0a syntax where different partition letters are treated as being on the samedisk drive. Partitions layered on top of an LSM device may not follow this naming convention. In this case unique pass numbers in /etc/fstab may be used to sequence fsck checks.

fstab(4) Reference Page Update

userquota [=filename] and groupquota [=filename]

If quotas are to be enforced for users or groups, one or both of the options must be specified. If userquota is specified, user quotas are to be enforced. If groupquota is specified, group:

OLD> quotas are to be enforced.

NEW> quotas are to be enforced (also see quotaon and quotaoff(8)).

OLD> For UFS file systems, the sixth field (fsck) is used by the fsck command to determine the order in which file system checks are done at reboot time. For the root file system, specify 1 in the fsck field. For other UFS file systems, specify 2 or higher in the fsck field. Each UFS file system should have a unique fsck value.

NEW> For UFS file systems, the sixth field (pass number) is used by the fsck and quotacheck commands to determine the order in which file system checks are done at reboot time. For the root file system, specify 1 in the fsck field. For other UFS file systems specify 2 or higher in the pass number field.

OLD> For AdvFS filesets, the sixth field is a pass number field that allows the quotacheck command to perform all of the consistency checks needed for the fileset. For the root file system, specify 1 in the fsck field. Each AdvFS fileset in an AdvFS file domain should have a unique fsck value, which should be 2 or higher.

NEW> For AdvFS filesets, the sixth field is a pass number field that allows the quotacheck command to perform all of the consistency checks needed for the fileset. For the root file system, specify 1 in the fsck field. For other AdvFS file systems specify 2 or higher in the pass number field.

OLD> File systems that are on the same disk are checked sequentially, but file systems on different disks are checked at the same time to utilize parallelism available in the hardware. If the sixth field is not present or zero, a value of 0 is returned and the fsck command assumes that the file system does not need to be checked.

NEW> File systems that are on the same disk or domain are checked sequentially, but file systems on different disks or domains but with the same or greater than 1 pass number are checked at the same time to utilize parallelism available in the hardware. When all the file systems in a pass have completed their checks, then the file systems with the numerically next higher pass number will be processed.

NEW> The UFS per disk drive logic is based on the

/dev/disk/dsk0a syntax where different partition letters are treated as being on the same disk drive. Partitions layered on top of an LSM device may not follow this naming convention. In this case unique pass numbers may be used to sequence fsck and quotacheck processing. If the sixth field is not present or zero, a value of 0 is returned and the fsck command assumes that the file system does not need to be checked.

1.6 Release Notes for Patch 476.00

Visual Threads users will need to upgrade to the latest version of Visual Threads in order for the race detection rules to work. The Visual Threads upgrade is available from `http://www.tru64unix.compaq.com/visualthreads` and will be available in the next Developers' Tooklit Supplement.

1.7 Release Note for Patch 315.00

This is a release note for the Enhanced Round Robin Sequential Read Patch.

If the system configurable parameter `lsm:lsm_V_ROUND_enhanced` is `set` (value = 1) the enhanced read round robin policy is activated. This new policy stores the last block accessed by the previous I/O request. When returning for another block in round robin (`V_ROUND`) mode, that value is compared to the current read. If it is within a predefined, user-configurable value (`lsm:lsm_V_ROUND_enhance_proximity`), then the same plex is used. Otherwise the next plex is used as for a normal round robin behavior.

The two new additional tunable parameters are `lsm_V_ROUND_enhanced` set to 1 by default (`V_ROUND` read is activated) and `lsm_V_ROUND_enhance_proximity` is set to 512 by default.

Append any tuning changes to `/etc/sysconfigtab`. See the TUNING notes below for a description of the new `lsm_V_ROUND_enhanced` and `lsm_V_ROUND_enhance_proximity` tunables. These tunables are configured in the `lsm` stanza. For example:

```
lsm:

lsm_V_ROUND_enhanced = 1

lsm_V_ROUND_enhance_proximity = 1024
```

Note

If you already have an `lsm` stanza in your `sysconfigtab` file, add the two `lsm_V_ROUND` entries.

TUNING

The purpose of this patch is to increase performance with sequential reads. This patch introduces a new enhanced round robin mode where the last block read is now compared to the next block to read and a check is added to see if last block number-next block number is less than or equal to `lsm_V_ROUND_enhance_proximity`. If it is, read from the same plex. This is to attempt to hit the disk cache, and so increase performance.

The relevant tunable variables are as follows:

`lsm_V_ROUND_enhanced`

This variable activates the new enhanced round robin read policy if it is set to TRUE (1). Otherwise the policy is deactivated.

DEFAULT = 1

lsm_V_ROUND_proxmity

This variable provides the proximity in which the last read and new read most lie in an attempt to read data from the disk's cache by reading from the same plex. The variable can be adjusted from 0 to 4096.

DEFAULT = 512

1.8 Release Note for Patch 351.00

For more information about the functionality provided and special installation instructions related to this patch, please refer to the online README file located at:

http://www.service.digital.com/patches/

From this URL directory, click on the following link:

duv40fwlseco2.README

Note

It may be necessary to navigate additional directories below this top level URL to find the specific README file related to this patch.

1.9 Release Note for TruCluster DRD Workaround

Adding a new member to an existing cluster will fail under the following conditions:

- The cluster is configured with a large number of DRDs.
- You are performing a rolling upgrade from TruCluster V1.5 to V1.6.
- The ASE data base has not been updated to the V1.6 structure.

To work around this problem, you must update the data base using the Enable ASE V1.6 functionality option from the Managing the ASE menu on the existing member prior to attempting to add the new member. Thus, the new member will be added with a V1.6-type ASE data base and will proceed successfully.

A patch will be in released in the near future.

1.10 Release Note for TCR Patch 30.00

If you are only installing TCR patches, you MUST rebuild the kernel and reboot the machine for the changes to take effect. If removing only TCR patches, you MUST also rebuild the kernel and reboot the machine for the changes to take effect.

2

Summary of Base Operating System Patches

This chapter summarizes the base operating system patches included in Patch Kit-0004.

Table 2–1 lists patches that have been updated.

Table 2–2 provides a summary of patches.

Table 2–1: Updated Base Operating System Patches

Patch IDs	Change Summary
Patches 342.00, 343.00, 350.00, 353.00, 355.00, 357.00, 358.00, 361.00, 373.00, 378.00, 381.00, 390.00, 395,00, 396.00, 400.00, 402.00, 405.00, 406.00, 409.00, 416.00, 417.00, 422.00, 431.00, 434.00, 435.00, 437.00, 443.00, 461.00, 465.00, 467.00, 468.00, 469.00, 474.00, 475.00	New
Patches 5.00, 184.00	Patch 341.00
Patch 4.00	Patch 344.00
Patches 189.00, 190.00, 191.00, 193.00, 214.00, 345.00, 346.00, 347.00, 348.00	Patch 349.00
Patches 212.00, 340.00, 223.00	Patch 351.00
Patches 217.00, 219.00, 354.00	Patch 356.00
Patches 64.00, 74.0, 199.00, 200.00, 220.00, 352.00	Patch 359.00
Patch 374.00	Patch 406.00
Patch 428.00	Patch 431.00
Patch 78.00	Patch 439.00
Patches 15.00, 23.00, 24.00, 25.00, 120.00, 142.00, 145.00, 156.00, 175.00, 376.00, 410.00	Patch 440.00
Patches 45.00, 316.00	Patch 444.00
Patch 225.00	Patch 447.00
Patches 318.00, 231.00, 394.00	Patch 448.00
Patches 90.00, 168.00, 269.00	Patch 449.00
Patches 108.00, 325.00	Patch 450.00
Patch 94.00	Patch 451.00
Patches 42.00, 276.00	Patch 452.00
Patches 44.00, 267.00, 277.00, 290.00, 333.00, 363.00, 367.00	Patch 454.00

Table 2–1: Updated Base Operating System Patches (cont.)

Patches 9.00, 10.00, 13.00, 27.00, 30.00, 55.00, 96.00, 99.00, 102.00, 106.00, 107.00, 110.00, 116.00, 117.00, 122.00, 126.00, 129.00, 141.00, 146.00, 160.00, 164.00, 174.00, 31.00, 178.00, 81.00, 112.00, 134.00, 224.00, 230.00, 238.00, 239.00, 244.00, 24800, 255.00, 257.00, 259.00, 265.00, 270.00, 291.00, 294.00, 303.00, 307.00, 310.00, 312.00, 317.00, 118.00, 33.00, 49.00, 50.00, 51.00, 52.00, 88.00, 100.00, 115.00, 121.00, 54.00, 161.00, 331.00, 227.00, 234.00, 258.00, 261.00, 264.00, 280.00, 292.00, 300.00, 321.00, 176.00, 329.00, 229.00, 83.00, 246.00, 131.00, 73.00, 58.00, 180.00, 210.00, 288.00, 304.00, 320.00, 326.00, 16.00, 130.00, 332.00, 152.00, 263.00, 92.00, 149.00, 150.00, 181.00, 250.00, 278.00, 305.00, 86.00, 324.00, 132.00, 360.00, 362.00, 365.00, 366.00, 368.00, 369.00, 370.00, 371.00, 372.00, 375.00, 377.00, 379.00, 380.00, 382.00, 388.00, 389.00, 391.00, 392.00, 393.00, 397.00, 398.00, 399.00, 403.00, 404.00, 411.00, 412.00, 413.00, 414.00, 418.00, 423.00, 424.00, 425.00, 426.00, 429.00, 430.00, 432.00, 433.00, 441.00, 442.00, 445.00, 446.00, 453.00, 455.00, 459.00, 460.00, 462.00, 327.00, 286.00, 385.00, 464.00, 463.00, 415.00	Patch 456.00
Patches 79.00, 125.00, 138.00, 172.00, 91.00, 177.00, 173.00, 247.00, 266.00, 408.00, 48.00, 438.00, 87.00	Patch 457.00
Patches 12.00, 85.00	Patch 458.00
Patch 63.00	Patch 470.00
Patch 334.00	Patch 471.00
Patches 203.00, 338.00, 472.00	Patch 473.00
Patch 71.00	Patch 476.00

Table 2–2: Summary of Base Operating System Patches

Patch IDs	Abstract
Patch 2.00 OSF440CDE-002	**Patch:** Security (SSRT0571U) **State:** Supersedes patch OSF440CDE-001 (1.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability. • Fixes a problem where the CDE mail interface (dtmail) does not display the date and time of mail messages in the Message Header list when the time zone is set to certain time zones such as GB-Eire.
Patch 3.00 OSF440CDE-003	**Patch:** Security (SSRT0585U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 7.00 OSF440DX-001	**Patch:** dxcalendar Reminder Displays Through dxpause Screen **State:** Existing This patch fixes the problem where the dxcalendar reminder displays through the pause screen (dxpause) and remains on the top of the pause window.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 8.00 OSF440-010	**Patch:** Fix For POP Mail Handler **State:** Existing This patch corrects the following: • Netscape Mail clients are unable to access their mailboxes after an initial session. The /usr/spool/pop/username.lock file is left over and must be removed manually. • The POP mail handler fails to properly rename its temp file after receiving a quit command.
Patch 11.00 OSF440-013	**Patch:** Security (SSRT0596U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 19.00 OSF440-020	**Patch:** Fix For yacc **State:** Existing This patch fixes a problem in yacc that causes it to generate parse tables that result in the parser not executing a user-specified error recovery action. If a yacc specification worked in Version 3.2 and no longer works in Version 4.0, this may be the problem.
Patch 20.00 OSF440-022	**Patch:** Cannot Use ipcs Cmd On System Not Booted With vmunix **State:** Existing This patch corrects a problem that prevents a user from using the ipcs command on a system whose kernel has been booted from a file that is not /vmunix.
Patch 21.00 OSF440-023A	**Patch:** Fix For XTI And DECnet/OSI **State:** Supersedes patch OSF440-016A (14.00) This patch corrects the following: • Fixes a problem in which an application using the X/Open Transport Interface (XTI) and the DECnet/OSI transport provider is unable to disconnect a rejected request. • Fixes a streams problem in libxti. The t_getprotaddr() function will cause a memory core dump if either of its second or third argument is NULL.
Patch 28.00 OSF440-030	**Patch:** Security (SSRT0556U) **State:** Existing A potential security vulnerability has been discovered where,under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability.
Patch 32.00 OSF440-034	**Patch:** mkdir -p Not Returning Error **State:** Existing This patch fixes a problem with the mkdir -p command. mkdir -p would not return an error if the last component in the pathname already exists.
Patch 34.00 OSF440-004	**Patch:** Fix For kio Subsystem Panic **State:** Existing This patch fixes a panic seen when accessing the kio subsystem (such as with consvar) with improper arguments. The panic was caused by a kernel double-free, and would most likely be seen as a corruption in either the 64- or 96-byte bucket (buckets 2 and 16).

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 36.00 OSF440-041	**Patch:** volrootmir -a Cmd Fails **State:** Existing This patch fixes a problem where the LSM command volrootmir -a fails if the source and target disks are not the same type.
Patch 37.00 OSF440-042	**Patch:** volrecover Not Returning Failed Status Code **State:** Existing This patch corrects a problem in which a failure of the volrecover utility will not return a failed status code.
Patch 38.00 OSF440-043	**Patch:** quotaon Returns Incorrect Error Status **State:** Existing This patch fixes a problem in which the quotaon command returned an incorrect error status if the file system did not exist.
Patch 40.00 OSF440-046	**Patch:** binmail Delivers Only Partial Messages **State:** Existing This patch fixes binmail to prevent partial delivery of mail messages when disk quota is reached.
Patch 41.00 OSF440-047A	**Patch:** Fix For nroff Y2K Problem **State:** Existing This patch fixes a Y2K problem with the nroff text formatter in which the years after 1999 are translated to be 19xxx with xxx being the number of years that have passed since 1900. In this case, the year 2010 displays as 19110.
Patch 43.00 OSF440-049	**Patch:** Fix For XTI Over TCP/IP **State:** Existing This patch fixes a problem with XTI over TCP/IP when tcp_sendspace and tcp_recvspace have been decreased to 1 K. When sending 4 K data (using t_snd), the call is successful but no data has been sent and no message is returned.
Patch 46.00 OSF440-052A	**Patch:** Shared Library Fix For curses-based Applications **State:** Existing The keymap used with curses functionality was not in sync with the table contained in the term.h header file. This change corrects that and enables several nonfunctioning keys in curses-based applications.
Patch 60.00 OSF440-008	**Patch:** Fix For spo_misc_errors errlog Entries **State:** Existing This patch fixes the cause of the spurious spo_misc_errors errlog entry on 4100 class systems.
Patch 61.00 OSF440X11-001	**Patch:** Enhancement For makedepend Utility **State:** Existing This patch increases the maximum number of files that one file can depend on in the makedepend utility from 1024 to 4096.
Patch 66.00 OSF440-023B	**Patch:** libxti/libtli Static Library Fix **State:** Supersedes patch OSF440-016B (65.00) This patch corrects the following: • Fixes a problem in which an application using the X/Open Transport Interface (XTI) and the DECnet/OSI transport provider is unable to disconnect a rejected request. • Fixes a streams problem in libxti. The t_getprotaddr() function will cause a memory core dump if either of its second or third argument is NULL.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 67.00 OSF440-033B	**Patch:** mount Cmd Sometimes Kills Other Processes **State:** Existing This patch fixes a problem with the mount command where it sometimes kills other processes.
Patch 68.00 OSF440-047B	**Patch:** nroff Incorrectly Translates Years After 1999 **State:** Existing This patch fixes a Y2K problem with the nroff text formatter in which the years after 1999 are translated to be 19xxx with xxx being the number of years that have passed since 1900. In this case, the year 2010 displays as 19110.
Patch 69.00 OSF440-052B	**Patch:** Static Library Fix For curses-based Applications **State:** Existing The keymap used with curses functionality was not in sync with the table contained in the term.h header file. This change corrects that and enables several nonfunctioning keys in curses-based applications.
Patch 75.00 OSF440-060B	**Patch:** chvol Read & Write Transfer Size Increased **State:** Existing This patch corrects the following: • AdvFS volumes were not setting the default I/O byte transfer size to the preferred size reported by the disk drives. • AdvFS chvol read and write transfer size range was increased. • The read-ahead algorithm was modified to improve performance under certain conditions.
Patch 76.00 OSF440-001	**Patch:** Fix for simple lock panic **State:** Existing This patch fixes a system panic with the following panic string: simple_lock: time limit exceeded
Patch 80.00 OSF440-103	**Patch:** Fix for cdfs file system **State:** Existing This patch fixes a problem with the cdfs file system. The default a partitions are being made incorrectly by the disk driver for ISO-9660 CDs causing data corruption when reading beyond the end of a partition. Only new and non-DEC CD-ROM drives are affected.
Patch 82.00 OSF440-106	**Patch:** Fix for system crash **State:** Existing This patch fixes a problem in which the system was consistently crashing by pressing keys during the transition from firmware callback to OS console handling.
Patch 93.00 OSF440-117	**Patch:** Fix for kdbx **State:** Supersedes patch OSF440-104B (201.00) This patch corrects the following: • Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash. • Fixes a problem with kdbx. The trace command was showing all threads of a process when using the option that should show only selected threads.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 101.00 OSF440-126	**Patch:** Fix for prof -pixie -asm command **State:** Supersedes patch OSF440-122B (202.00) This patch corrects the following: • Fixes the name demangling for the tools that print symbol table names generated by the C++ V6.2 compiler. This problem will only occur for most C++ objects compiled with the ANSI options. • Fixes a problem where prof -pixie -asm would dump core if the executable being profiled contains extremely long symbol names.
Patch 104.00 OSF440-130	**Patch:** System hang prevents rlogins or telnets **State:** Existing This patch fixes a problem where systems could hang in the audit code, preventing rlogins or telnets into it.
Patch 105.00 OSF440-131A	**Patch:** Fix for class_admin class_daemon problem **State:** Existing This patch fixes a class_admin/class_daemon problem. When a PID is added to a class it cannot be removed from the class scheduler until the process terminates or the class_scheduler has been stopped.
Patch 119.00 OSF440-145	**Patch:** System hang occurs in I2c code **State:** Existing This patch fixes a intermittent hang occurring in the I2c code. This hang is most commonly seen on the DS10 workstation.
Patch 124.00 OSF440-150A	**Patch:** libots3 shared run-time library fix **State:** Existing The failure to check the return status after certain system calls caused a problem in the libots3 run-time library. The libots3 run-time library supports OpenMP parallel applications.
Patch 127.00 OSF440-153	**Patch:** Security (SSRT0583Z) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 128.00 OSF440-154	**Patch:** Fix and update for sys_check utility **State:** Existing This patch provides bug fixes to the sys_check utility and updates the sys_check to Version 114.
Patch 135.00 OSF440-021	**Patch:** Fix for ar command **State:** Existing This patch eliminates the previous limitation on the maximum number of external symbols that could be handled by the ar command.
Patch 139.00 OSF440-037	**Patch:** Fix for lock-terminate system panic **State:** Existing This patch fixes a kernel problem, where proper locking/reference count management was not being performed. This could result in a "lock-terminate: lock held" system panic.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 140.00 OSF440-038	**Patch:** Fixes a problem with the newfs command **State:** Supersedes patch OSF440-121 (97.00) This patch corrects the following: • Fixes invalid malloc message in mfs. • Fixes a problem with the newfs command. When the newfs -N command was run on a mounted file system, it returned an error message similar to the following: newfs: /dev/rrz0c: is marked in the disklabel as in use by: 4.2BSD
Patch 144.00 OSF440-064	**Patch:** Fix for NFS problems **State:** Existing This patch corrects the following: • When starting or stopping NFS, NFS was not checking for NFS daemons running. • rpc.pcnfsd was causing core dumps when receiving a SIGTERM signal.
Patch 148.00 OSF440-069	**Patch:** Fix for rsh hang **State:** Existing This patch fixes rsh(1) hanging forever in select().
Patch 153.00 OSF440-074	**Patch:** Fixes a problem within the SCSI and tape subsystems **State:** Existing This patch fixes a problem within the SCSI and tape subsystems, in which an expression was not being evaluated properly.
Patch 154.00 OSF440-075	**Patch:** Fixes restart detection problem with proplistd **State:** Supersedes patch OSF440-063 (57.00) This patch corrects the following: • Corrects several NFS problems: – Fixes a problem where NFS does not update mtime and atime for special files and named pipes. – Fixes a problem that can cause an NFS client application to hang, or causes a "lock already owned by thread" panic when lockmode=4. – Fixes a problem where incorrect NFS client locking caused a KFM panic. – Fixes a problem where NFS clients may hang in the uninterruptable state. • Fixes a restart detection problem with the proplistd daemon. Prior to this fix, when mounting a relocated ASE NFS service with property lists, clients did not detect that the proplistd RPC port number had changed. Clients continued to use the proplistd RPC port number of the old ASE cluster member.
Patch 159.00 OSF440-080	**Patch:** Fix for system hang with inetd **State:** Existing This patch fixes a problem in which a system can hang when inetd tries to start a daemon listed in inetd.conf, which is not installed on the system. This can occur when a user attempts to telnet to the port reserved for the nonexistent daemon.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 162.00 OSF440-083	**Patch:** Fix for unresolved symbol:scc_configure message **State:** Existing This patch fixes a problem in which systems that use Compaq Tru64 UNIX and install DECnet/OSI and WDD would get the following error message when attempting to build a kernel: unresolved symbol:scc_configure
Patch 167.00 OSF440-089	**Patch:** Fix for vdump core dump problem **State:** Existing This patch fixes a problem where the vdump program would dump core with the following message: nnnn Resources lost(coredump)
Patch 169.00 OSF440-090	**Patch:** Fix for crontab -e user command **State:** Existing This patch fixes a problem with crontab in which, when root runs crontab -e user, the user's crontab file is edited and saved, but is not re-read by the cron daemon. Instead, root's crontab file is re-read.
Patch 170.00 OSF440-091	**Patch:** Fixes a problem with the stdhosts command **State:** Existing This patch fixes a problem with the stdhosts command when the file processed has lines longer than 256 characters. The error message "stdhost:malformed line ignored" is displayed.
Patch 179.00 OSF440-192	**Patch:** Fix for panics on AlphaServer GS140/GS60 systems **State:** Supersedes patch OSF440-002 (18.00) This patch corrects the following: • Resolves corrupt EV6 binary error log entries for IOP detected UDE (Uncorrectable Data Error) packets on AlphaServer 8200/8400 platforms. • Fixes a problem on some AlphaServer GS140/GS60 configurations where a simple lock timeout or TB shoot ack timeout panic may occur.
Patch 182.00 OSF440CDE-010	**Patch:** Fix for X server color map problem **State:** Existing This patch fixes a problem where there were no available colors in the X server's color map after the CDE screen lock was displayed.
Patch 183.00 OSF440CDE-011	**Patch:** Security (SSRT0614U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 185.00 OSF440CDE-008	**Patch:** Security (SSRT0600U) **State:** Supersedes patch OSF440CDE-006 (6.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. • Fixes a problem where dtlogin may incorrectly set the permissions of /var to 775. It also fixes a problem where dtlogin may incorrectly set the umask to 002 for csh users.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 186.00 OSF440CDE-009A	**Patch:** Fix for dxaccounts error message **State:** Existing This patch fixes a problem where the Account Manager application, dxaccounts, gets a "BadPixmap" error when selecting an account after the "View Preferences" "Display Icons By Name" option has been selected.
Patch 187.00 OSF440DX-002	**Patch:** diskconfig fails when creating an AdvFS partition **State:** Supersedes patch OSF440DX-007 (192.00) This patch corrects the following: • Fixes a problem with the diskconfig utility where ri type disks were not correctly recognized. • Fixes a problem where, when creating an AdvFS partition, the disk configuration utility (/usr/sbin/diskconfig) failed with the error: Error in Tcl Script Error: can't read dskdir: no such variable
Patch 188.00 OSF440DX-003	**Patch:** Compaq SCSI SNMP sub-agent returns incorrect info **State:** Existing This patch fixes a problem that causes the Compaq SCSI SNMP subagent (cpq_mibs) to often return incorrect SCSI CD-ROM and tape devices model information, which results in invalid information displaying on the Insight Management Web pages.
Patch 194.00 OSF440DX-009	**Patch:** Security (SSRT0612U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 196.00 OSF440X11-006	**Patch:** XDMCP Indirect queries do not work **State:** Existing This patch fixes a problem in the X Display Manager (xdm) where XDMCP Indirect queries do not work.
Patch 198.00 OSF440X11-008	**Patch:** X server crashes when viewing TIFF images **State:** Existing This patch fixes a problem where viewing certain TIFF images with an image viewer crashed the X server.
Patch 204.00 OSF440-150B	**Patch:** libots3 static run-time library fix **State:** Existing This patch corrects the failure to check the return status after certain system calls caused a problem in the libots3 run-time library. The libots3 run- time library supports OpenMP parallel applications.
Patch 205.00 OSF440CDE-009B	**Patch:** Fix for dxaccounts BadPixmap error **State:** Existing This patch fixes a problem where the Account Manager application, dxaccounts, gets a "BadPixmap" error when selecting an account after the "View Preferences" "Display Icons By Name" option has been selected.
Patch 209.00 OSF440-131B	**Patch:** Static library fix for libclass.a **State:** Existing This patch fixes a class_admin/class_daemon problem. When a PID is added to a class it cannot be removed from the class scheduler until the process terminates or the class_scheduler has been stopped.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 211.00 OSF440CDE-012	**Patch:** Security (SSRT0615U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 213.00 OSF440CDE-015	**Patch:** New windows are visible when screen is locked **State:** Existing This patch fixes a problem where, when running the Common Desktop Environment (CDE) on a system with more than one graphics card and monitor (multihead), new windows were sometimes visible when the screen was locked.
Patch 215.00 OSF440DX-012	**Patch:** checklist utility does not provide scroll bar **State:** Existing This patch fixes a problem where the checklist utility did not provide a scroll bar on higher resolution displays (1600x1200).
Patch 216.00 OSF440DX-013	**Patch:** diskconfig may display incorrectly **State:** Existing This patch fixes a problem where the Disk Configuration Manager application, diskconfig, displayed incorrectly on some non-Compaq X servers. The font used for menu items was incorrect so that the menus contained random symbols instead of text.
Patch 218.00 OSF440X11-011A	**Patch:** X Server may generate an Invalid Pixmap Error **State:** Supersedes patch OSF440X11-002A (62.00) This patch corrects the following: • Fixes a problem with Motif Drag-and-Drop where, if a parent drop site was unregistered before a child drop site, subsequently unregistering the child drop site would cause a segmentation fault. • Fixes a problem with the toggle button where, if a display is closed and reopened, then the X Server may generate an "Invalid Pixmap Error".
Patch 221.00 OSF440X11-017	**Patch:** Fixes problem on systems with a Powerstorm 4D10T **State:** Existing This patch fixes a problem where, on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the X server did not draw lines correctly.
Patch 222.00 OSF440X11-018A	**Patch:** Fixes memory leak in X Toolkit library **State:** Supersedes patch OSF440X11-005A (195.00) This patch corrects the following: • Fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt). • Fixes a memory leak in the X Toolkit library (libXt). This memory leak could be seen by applications that create and destroy many Motif ScrolledWindow widgets
Patch 232.00 OSF440-172	**Patch:** Fix for lex command **State:** Existing This patch fixes a problem in lex that causes it to generate incorrect tables. This results in the lexical analyzer failing to recognize some kinds of regular expressions involving exclusive start states.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 233.00 OSF440-173	**Patch:** Fix for ris script **State:** Existing This patch corrects the following problems with the /usr/sbin/ris script: • It incorrectly queried the user for a gateway to be used to serve a specific client when no gateway was required. • It could fail if no default route had been established.
Patch 236.00 OSF440-178	**Patch:** Fixes a problem that occurs when using ftp **State:** Existing This patch fixes a problem that occurs when using ftp. When mget or nlist specify a filename with metacharacters and the mode is ASCII, the file is returned with <LF> as the end-of-file separator. With this patch, files are returned with <CR><LF> as the end-of-file separator.
Patch 237.00 OSF440-179	**Patch:** defragment incorrect reports large free space holes **State:** Supersedes patch OSF440-029 (26.00) This patch corrects the following: • Fixes a problem with the defragment command, where the -V option is not being parsed properly. • Fixes the defragment program to properly report on extremely large (>4.3GB) freespace holes. Previously it would report Free space percentages larger than 100% and would add these large holes to the smallest range (<100K) instead of the largest range (>10M) where they belong.
Patch 241.00 OSF440-184	**Patch:** Fix for crashes seen on ASE or TruCluster systems **State:** Supersedes patches OSF440-113 (89.00), OSF440-177 (235.00) This patch corrects the following: • Fixes system crashes seen on ASE or TruCluster systems when changing the network interfaces. The stack is not informative and the panic may be "trap: illegal instruction," or "kernel memory fault." • Corrects a problem where ICMP redirect packets can modify the default route.
Patch 242.00 OSF440-185	**Patch:** Fix for news command **State:** Existing This patch fixes a problem in which the news command fails due to the appending of additional characters to file names in the /usr/news directory.
Patch 243.00 OSF440-186	**Patch:** Fix for rpc.statd hang **State:** Existing This patch fixes a problem where rpc.statd hangs as it tries to notify dead remote systems.
Patch 245.00 OSF440-188	**Patch:** Cannot restore system configured with backplane RAID **State:** Existing This patch fixes a problem where, when the user attempts to restore to a system configured with backplane RAID, btextract fails.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 252.00 OSF440-199	**Patch:** nm command causes core dump **State:** Supersedes patch OSF440-122A (98.00) This patch corrects the following: • Fixes the name demangling for the tools that print symbol table names generated by the C++ V6.2 compiler. This problem will only occur for most C++ objects compiled with the ANSI options. • Fixes a problem with nm that can cause a core dump when the LANG environment variable is set.
Patch 256.00 OSF440-205	**Patch:** mkfdmn command does not report errors **State:** Existing This patch corrects a problem that resulted in the mkfdmn command not reporting errors if you attempted to create a volume with a name that is more than 31 characters long.
Patch 260.00 OSF440-211	**Patch:** Fix for mailsetup command **State:** Existing This patch fixes a problem of not completing mailsetup if the hostname ends with 0 (zero). The error message produced is: Error creating /var/adm/sendmail/.cf: exiting
Patch 262.00 OSF440-217	**Patch:** lprsetup command sets up printers incorrectly **State:** Existing This patch fixes a problem where the lprsetup command would incorrectly set up certain types of printers, such as the hp1120c, hp4000tn, or hp61.
Patch 268.00 OSF440-225	**Patch:** NFS system using a TCP connection may crash **State:** Supersedes patches OSF440-135 (109.00), OSF440-140 (114.00) This patch corrects the following: • Fixes a system hang problem due to a bug in the NFS write gathering code. The code does not fully synch all writes. • Fixes a problem where applications on V4.0F systems can hang, looping in readdirplus(). • Fixes a problem in which an NFS system using a TCP connection can crash.
Patch 271.00 OSF440-228	**Patch:** ftp command causes core dump problem **State:** Existing This patch fixes a coredump problem with ftp(1) when a .netrc file contains an invalid macdef (macro definition).
Patch 272.00 OSF440-229	**Patch:** fverify command has problems creating directories **State:** Existing This patch fixes a problem with the fverify -n flag creating directories.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 281.00 OSF440-245	**Patch:** Fix for tmv2_notify_cbf problem **State:** Supersedes patches OSF440-006 (53.00), OSF440-165 (226.00), OSF440-234 (273.00) This patch corrects the following: • Fixes a panic that occurs when KZPSA resources are not available to re-enable a channel or a device after a bus reset. The panic string is: panic("(spo_process_rsp) ran out of memory!") • Fixes a problem with the KZPSA driver. A timer is not being canceled causing a panic with the following error message: xpt_callback: callback on freed CC • Fixes a problem in which the system can panic with the following message: KZPSA PANIC SPO_RET_CARRIER:CARRIER NOT IN USE • Fixes a problem with tmv2_notify_cbf messages being logged from KPBSA adapters and creating very large binary.errlog files in a clustered environment.
Patch 284.00 OSF440-248	**Patch:** Problem with unit attention status being missed **State:** Supersedes patch OSF440-100 (77.00) This patch corrects the following: • Fixes the problem where the tapex -L command would report failure when run on certain devices. The failure would be reported when the command was run on certain TLZ09 devices, depending on the firmware. • Fixes a problem that could result in unit attention status being missed.
Patch 285.00 OSF440-249	**Patch:** bprelay daemon does not work properly **State:** Supersedes patches OSF440-079 (158.00), OSF440-201 (253.00), OSF440-246 (282.00) This patch corrects the following: • Adds an error message to DHCP to inform a user that they may be using an outdated database. The message also points to the README for database conversion instructions. • Fixes a problem of the joind daemon not appending the hostname to the load file specified in the bf flag in the /etc/bootptab file. • Fixes a problem in which joind does not listen on interfaces configured with DECnet and returns "unaligned access" messages. • Fixes a problem in which bprelay does not work properly and displays the following error message bprelay[658]: can't find interface which received packet
Patch 295.00 OSF440-260	**Patch:** Fix for unaligned access panic in dli_input **State:** Existing This patch fixes an unaligned access panic in dli_input.
Patch 296.00 OSF440-261	**Patch:** Fix for compress utility **State:** Existing This patch corrects a problem with the (un)compress utility that could result in either an incomplete compressed file and loss of the original uncompressed file, or an incomplete uncompressed file and loss of the original compressed file.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 297.00 OSF440-262A	**Patch:** Fix for voldisksetup, voldiskadd, and newfs **State:** Existing This patch fixes problems with the voldisksetup, voldiskadd, or newfs commands. Each will report device errors while checking for overlapping partitions where there is no overlap on that particular device.
Patch 298.00 OSF440-263	**Patch:** Upgrade to Gigabit Ethernet driver version 1.0.12 **State:** Existing This patch is an upgrade to the Gigabit Ethernet driver Version 1.0.12 that fixes various performance problems.
Patch 299.00 OSF440-264	**Patch:** Fix for update installation hang **State:** Existing This patch fixes a problem in which a hang can occur during update install.
Patch 301.00 OSF440-266	**Patch:** System panics when accessing defective CDROM **State:** Supersedes patches OSF440-044 (39.00), OSF440-087 (165.00), OSF440-167 (228.00) This patch corrects the following: • Fixes a problem where a system panic will occur when accessing an ISO9660 format CD-ROM. • Fixes a problem with CDFS. Data corruption occurs when reading beyond the end of a partition. • Fixes a problem in which the system may memory fault if the TCR/ASE server no longer had access to the CD-ROM device. • Fixes a problem where the system can panic with the panic string "secsize_resid < d_reclen" when accessing a defective CD-ROM.
Patch 302.00 OSF440-267	**Patch:** Problem with NetRAIN and HE155 (FORE) ATM cards **State:** Existing This patch fixes a NetRAIN problem when using HE155 (FORE) ATM cards. NetRAIN will fail when configuring LANE to join ELANs.
Patch 306.00 OSF440-271	**Patch:** Fixes Standards namespace pollution problem **State:** Existing This patch corrects some Standards namespace pollution.
Patch 308.00 OSF440-273	**Patch:** Corrects an NIS client problem **State:** Existing This patch corrects a problem where an NIS client has a different shell listed for an NIS user than does the server. When the users tried to change their NIS passwords, the password change failed, but the shell was updated.
Patch 309.00 OSF440-275	**Patch:** Provides collection tool used by sys_check utility **State:** Supersedes patch OSF440-258 (293.00) This patch corrects the following: • Provides the following changes to the sys_check utility: – Fixes the ra200info tool from core dumping. – Adds the sysconf program. • Fixes the following two problems with the collect information tool used by the sys_check utility: – A security hole where a user can become root. – collect cannot start at boot time due to incorrectly handling SIGHUP signal.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 311.00 OSF440-277	**Patch:** sysconfigdb incorrectly adds blank lines **State:** Existing This patch corrects a problem in which sysconfigdb would incorrectly add or delete blank lines to or from the target file.
Patch 313.00 OSF440-279	**Patch:** showfdmn may core dump **State:** Existing This patch fixes a problem in which advfs showfdmn would sometimes core dump.
Patch 314.00 OSF440-281	**Patch:** Fixes callback on freed CCB panics **State:** Supersedes patches OSF440-025 (136.00), OSF440-247 (283.00) This patch corrects the following: • Fixes callback thread blocking forever in isp_enable_lun. • Fixes assert wait in xpt_ccb_alloc panic. • Fixes a problem on configurations having multiple Qlogic 1020/1040 based SCSI controllers (for example KZPBAs) and multiple CPUs. The problem could result in stalled I/O. This could be seen as a performance degradation, command timeouts, or, in the worse cases, a system hang condition. • Fixes callback on freed CCB panics.
Patch 315.00 OSF440-282	**Patch:** Fixes performance problem on LSM mirrored volumes **State:** Existing This patch fixes a performance problem for round robin sequential reads on LSM mirrored volumes.
Patch 319.00 OSF440-287	**Patch:** Security (SSRT0592U) **State:** Supersedes patch OSF440-241 (279.00) This patch corrects the following: • Fixes a problem with rdist(1) that consumes huge amounts of memory, and when there are a lot of symlinks in the fileset, it can simply fail to fully populate the remote site or cause low-memory problems on the local machine. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 322.00 OSF440-290	**Patch:** sendmail core dumps when sending mime-encoded files **State:** Existing This patch fixes a problem where sendmail core dumped when trying to send certain 8-bit, mime-encoded files.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 323.00 OSF440-291	**Patch:** Various fixes for ALPHAVME320 systems **State:** Supersedes patch OSF440-108 (84.00) This patch corrects the following: • Fixes two problems on the ALPHAVME320 platform: – Data corruption in the VB Backplane driver. – No floppy support in the platform code. Following is the error message received during the boot when the floppy is configured at irq6: EBV16, invalid isa0 irq6 • Fixes three problems in the existing VB VME Backplane Driver running on AlphaVMExx platforms: – VB VME Backplane Driver does not configure when the sysconfigtab parameter, VB_MAXNODES, is less than 10. – VB VME Backplane Driver hangs and the nodes lose liveness when the sysconfigtab parameter, VB_MAXNODES, is equal to 2. – VB VME Backplane Driver Performance is unacceptable for customer applications.
Patch 330.00 OSF440-304	**Patch:** Fix for serial line hang **State:** Supersedes patch OSF440-007 (59.00) This patch corrects the following: • When using tip or any other method over the serial com lines to a receiver that sends frequent xoff/xon, characters are randomly repeated. • On a DECstation 2000/300, the second com port (tty01) does not get configured. An error message "ksh: /dev/tty01: cannot create" is displayed when the tty01 port is accessed. • Fixes serial line hang and enables halt switch on Eiger.
Patch 335.00 OSF440X11-011B	**Patch:** Fixes a problem with the toggle button **State:** Supersedes patch OSF440X11-002B (70.00) This patch corrects the following: • Fixes a problem with Motif Drag-and-Drop where, if a parent drop site was unregistered before a child drop site, subsequently unregistering the child drop site would cause a segmentation fault. • Fixes a problem with the toggle button where if a display is closed and reopened the X Server may generate an "Invalid Pixmap Error".
Patch 336.00 OSF440X11-018B	**Patch:** Static library fix (libXt) **State:** Supersedes patch OSF440X11-005B (206.00) This patch corrects the following: • Fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt). • Fixes a memory leak in the X Toolkit library (libXt). This memory leak could be seen by applications that create and destroy many Motif ScrolledWindow widgets.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 337.00 OSF440-168B	**Patch:** Fix for AdvFS property list handling **State:** Existing This patch corrects two problems in AdvFS property list handling: • Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf). • The get_proplist_entry function (used to disassemble the property list buffer returned by the getproplist system call) returned the incorrect name length on property list names longer than 127 characters.
Patch 339.00 OSF440-262B	**Patch:** voldisksetup incorrectly reports device errors **State:** Existing This patch fixes problems with voldisksetup, voldiskadd, or newfs commands. Each will report device errors while checking for overlapping partitions where there is no overlap on that particular device.
Patch 341.00 OSF440CDE-018	**Patch:** Fixes file permission problem for trashinfo file **State:** Supersedes patches OSF440CDE-005 (5.00), OSF440CDE-007 (184.00) This patch corrects the following: • Fixes a problem where the CDE File Manager (dtfile) sometimes left defunct processes. • Fixes a problem where the Common Desktop Environment (CDE) File Manager (dtfile) did not work correctly in restricted mode. • Fixes a problem in which file permissions allow any user to write to the /.dt/Trash/.trashinfo file.
Patch 342.00 OSF440CDE-019A	**Patch:** Security (SSRT0617U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 343.00 OSF440CDE-020A	**Patch:** Fix for the dtfile ICDE COSE tool **State:** New This patch fixes a problem in which dtfile ICDE COSE tool does not work when TMPDIR is defined as /ldata/disk_local/tmp. dtfile returns this error: /ldata/disk_local/tmp/sdtdbcache_AAAaadmma: Cross-device link /ldata/disk_local/tmp/sdtdbcache_BAAaadmma: Cross-device link Floating exception (core dumped)
Patch 344.00 OSF440CDE-021	**Patch:** Security (SSRT0580U) **State:** Supersedes patch OSF440CDE-004 (4.00) This patch corrects the following: • A potential security vulnerability has been discovered, where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. • Fixes a problem where the Common Desktop Environment (CDE) Application Manager did not recreate the list of application groups at login. After customizing the application groups, users would see the old groups instead of the new groups.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 349.00 OSF440DX-018	**Patch:** Fix for dxaccounts application **State:** Supersedes patches OSF440DX-004 (189.00), OSF440DX-005 (190.00), OSF440DX-006 (191.00), OSF440DX-008 (193.00), OSF440DX-010 (214.00), OSF440DX-014 (345.00), OSF440DX-015 (346.00), OSF440DX-016 (347.00), OSF440DX-017 (348.00) This patch corrects the following: • Fixes two situations in which the gui account management program (dxaccounts) will crash in a Enhanced Security client environment when attempting to copy an NIS user account. • Fixes the problem with the useradd, usermod, userdel commands removing the last entry of the /etc/passwd file when the last line of the /etc/passwd file does not end with the new line character (\n). • Fixes a problem where usermod -D can coredump if an NIS group entry contains a large number of users. • Fixes a problem in which the command usermod was not allowing any commas in the comment field when the current GECOS fields are filled. • Fixes a problem in which a duplicate user identifier (UID) is accepted at a second attempt even if the no-duplicat-user-identifier policy is set. • Updates the error message displayed when Account Manager fails to start due to the detection of an Account Manager lock file (/etc/.AM_is_running) on the system. • Fixes the problem in which a command uermod -D does not display the Expire date when it is set. • Fixes a problem in which dxaccounts does not allow the system manager to add NIS users when the system is running enhanced security. • Fixes the problem of enabling to change root's login/uid through cli/dxaccounts utilities. • Fixes a problem in which the dxaccounts application does not allow users to be added to groups with Group ID lower than the default minimum specified in the General Options dialog.
Patch 350.00 OSF440X11-020A	**Patch:** Shared library fix for svn widget **State:** New This patch fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 351.00 OSF440X11-021	**Patch:** Provides missing compose definitions **State:** Supersedes patches OSF440CDE-014 (212.00), OSF440CDE-017 (340.00), OSF440X11-019 (223.00) This patch corrects the following: • Adds the ISO8859-15 functionality to the main Xresource file on the system and to the specific dtlogin resource file. With these changes, X applications have ISO8859-15 locale support integrated directly into the application. • Adds Catalan (ISO8859-15) to the list of languages from which users can choose when logging in. The additional item identifies the Catalan Latin-9 locale, which supports the Euro currency sign. • Implements Xlocales definitions that allow X applications to run under the ISO8859-15 locales. Using ISO8859-15 locales allows users to enter and use newly defined ISO8859-based characters such as the Euro monetary symbol. • Provides missing compose definitions when in ISO8859-15 based locales for the scaron, Scaron, zcaron, and Zcaron characters.
Patch 353.00 OSF440X11-023	**Patch:** Fix for Turkish F keyboard problem **State:** New This patch fixes the Turkish F keyboard problem, where the character Ccedilla and ccedilla cannot be entered from the keyboard directly.
Patch 355.00 OSF440X11-025A	**Patch:** Various fixes for X font server **State:** New This patch fixes various problems with the X font server and with the X server's interaction with X font servers.
Patch 356.00 OSF440X11-026A	**Patch:** Core dump when using input method server **State:** Supersedes patches OSF440X11-010A (217.00), OSF440X11-013 (219.00), OSF440X11-024 (354.00) This patch corrects the following: • Fixes a problem in which ^C fails to work in dtterm when logged in to a 4.0E or 4.0F system using XDMCP. • Fixes a character input problem for non-Latin-1 keyboards. • Fixes a problem in which some 8-bit characters cannot be entered directly from the keyboard when the Caps Lock setting is on. • Prevents a potential core dump from the X11 library when running an input method server for Japanese, Chinese, or Korean.
Patch 357.00 OSF440X11-027	**Patch:** X server may core dump when using Multi-Buffering **State:** New This patch fixes a problem where the X server could core dump or get unaligned access errors when clients used the Multi-Buffering extension.
Patch 358.00 OSF440X11-028	**Patch:** X server incorrectly includes DPSExtension **State:** New This patch fixes a problem where the X server would include the Adobe Display PostScript extension (Adobe-DPS-Extension, DPSExtension) in its response to a ListExtensions request even though Display PostScript is not supported in Tru64 UNIX V4.0F.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 359.00 OSF440X11-029	**Patch:** Fixes synchronization and drawing problems **State:** Supersedes patches OSF440X11-004 (64.00), OSF440X11-007 (74.00), OSF440X11-009 (199.00), OSF440X11-015 (200.00), OSF440X11-016 (220.00), OSF440X11-022 (352.00) This patch corrects the following: • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the graphics board was not initialized properly and failed to work on power-up or when the X server was restarted. • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the X server does not draw lines correctly. • Provides the X server support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA) (also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB). • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the X server did not draw text correctly. • Fixes a problem where on systems with a PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card or a PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA), sometimes lines and images are not drawn correctly in scrolled windows. • Fixes synchronization and drawing problems in the X server for the PowerStorm 4D10T (ELSA GLoria Synergy, SN-PBXGK-BB) graphics card.
Patch 361.00 OSF440-296	**Patch:** chfile utility returns incorrect error code **State:** New This patch fixes a problem in which the chfile utility returns an incorrect error code.
Patch 373.00 OSF440-315	**Patch:** Processes hang waiting for I/O interrupts **State:** New This patch corrects the following: • Processes may hang due to waiting for I/O interrupts. • The SCU command set pages pcf will hang a system when ATAPI CDrom device is selected.
Patch 378.00 OSF440-321	**Patch:** Fixes kernel memory fault in procfs_get_s5_dir **State:** New This patch fixes a kernel memory fault in procfs_get_s5_dir.
Patch 381.00 OSF440-327	**Patch:** Security (SSRT0624U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 383.00 OSF440-329	**Patch:** Security (SSRT0636U) **State:** Supersedes patch OSF440-019 (17.00) This patch corrects the following: • Fixes a problem in which a BIND server may find that named will place a warning message in the daemon.log that was not previously seen. • Fixes a problem in which a BIND server writes files to the /etc/namedb directory instead of to the /var/tmp directory. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 384.00 OSF440-330	**Patch:** Fixes for verify command problems **State:** Supersedes patches OSF440-040 (35.00), OSF440-183 (240.00) This patch corrects the following: • This enhancement for the /sbin/advfs/verify utility allows it to detect loops in the list of free frags kept in the frags file. • Avoids corruption of a filesystem when verify runs with -r & -f flags on an active domain. Verify returns usage message when -r flag is used with either -f or -d. • Fixes the following /sbin/advfs/verify command problems: – verify fails to complete on a large number of files. – verify will core dump when an offset into mountd[] array that is used to pull out the fileset name is corrupted. – verify incorrectly reports errors on BMTs that have multiple extent records for domains created with the mkfdmn -p switch. – verify fails when lseeking on very large domains.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 386.00 OSF440-333	**Patch:** Miscellaneous print command fixes **State:** Supersedes patches OSF440-236 (275.00), OSF440-254 (289.00) This patch corrects the following: • When printing jobs, a timeout can occur after five minutes which causes some large print jobs to stop, then resume printing from the beginning of the print job. • When slave lpd daemons try to process jobs on the print queue, some of them can fail to obtain a lock on the lock file, and exit with an error. • Print jobs will print out twice. • A remote print job may fail to print, with the error message: lstat/open failed for dfA... no such file or directory • If a print job is printing, and the connection to the remote printer is lost, the print job does not resume printing after the connection is restored. • Sometimes, as sequence numbers wrap around from 999 to 000, job 000 gets submitted before, and prints before, job 999. • lpstat -u output is incorrect. • When using the I18N ya option, the queue daemon filters will terminate after 32 jobs. • Under certain circumstances, print jobs are terminated when printing to certain printers that are connected to a DECserver through TCP/IP. • When lpd reads any data from the printer that has not been read, for local and remote connections, the read-backs for remote connections cause an additional 2-second time out which may cause a job-submit failure on the job-number wraparound.
Patch 387.00 OSF440-334	**Patch:** Fix for invalid multibyte character processing logic **State:** Supersedes patch OSF440-053 (47.00) This patch corrects the following: • Fixes a problem where vi puts the server port into PASSALL MODE (where XON/XOFF is no longer effective). This creates garbage in the file. • Fixes the error handling when invalid multibyte sequences are encountered in the more, ex, and vi commands.
Patch 390.00 OSF440-339	**Patch:** OSF440-339 **State:** New This patch prevents /sbin/vold from dumping core during an execution of a volprint or other query command.
Patch 395.00 OSF440-344	**Patch:** mdir command displays year 2000 date incorrectly **State:** Existing This patch fixes a problem in which the mdir command displays the date incorrectly for the year 2000.
Patch 396.00 OSF440-345	**Patch:** Problem with DE500 interfaces using ML6694F PHY **State:** Existing This patch corrects a problem with some DE500 interfaces that use the Micro Linear ML6694F PHY.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 400.00 OSF440-349	**Patch:** NetRAIN devices fail to come up after rcinet restart **State:** Existing This patch fixes a problem of NetRAIN devices failing to come up after the rcinet restart command is entered.
Patch 401.00 OSF440-350	**Patch:** osf_boot fails to link in foreign kits **State:** Supersedes patches OSF440-139 (113.00), OSF440-230 (207.00), OSF440-231 (208.00), OSF440-195 (249.00) This patch corrects the following: • Fixes a problem where the linker (ld) would insert incorrect values for the symbols etext and _etext when building kernels larger than 4 MB. • This patch is needed to support the NHD2 (New Hardware Delivery Two) release. The NHD2 installation process modifies the system's linker and the osf_boot file. This patch preserves the modifications that NHD2 makes to the linker and the osf_boot file. • Fixes a problem where the linker (ld) could not read arguments longer than 1024 characters in input files. This also adds proper support for line continuation characters. • Addresses the failure of osf_boot to link in foreign kits with the following message: osf_boot: Not enough space to add '..... messages
Patch 402.00 OSF440-351	**Patch:** Fixes hang in shutdown process **State:** Existing This patch fixes a hang in the shutdown process ("shutdown now") of a system when a device has flow control switched off.
Patch 405.00 OSF440-354	**Patch:** Fixes a tftpd problem **State:** Existing This patch fxes a tftpd problem when responding to a broadcast read request and it adds the -b ption to control whether to respond to any broadcasts.
Patch 406.00 OSF440-355	**Patch:** Fixes a kernel memory fault when using ATM **State:** Supersedes patch OSF440-316 (374.00) This patch corrects the following: • Fixes a problem in the ATM atm_cmm_connect API routine when trying to create a VC. • Fixes a kernel memory fault when using ATM.
Patch 407.00 OSF440-356	**Patch:** System may panic when running ATM ELANs **State:** Supersedes patch OSF440-068 (147.00) This patch corrects the following: • Fixes a problem with the creation of multiple ATM ELANS. • Fixes a problem in which the system may panic with the error message "Unaligned kernel space access from kernel mode" when running ATM ELANs.
Patch 409.00 OSF440-358	**Patch:** Fixes a problem with NCR810 script **State:** Existing This patch fixes a problem with the NCR810 script that can cause the KZPAA/NCR810 to hang.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 416.00 OSF440-365	**Patch:** Extends max length of identifier for assembler **State:** Existing This patch resolves a problem that caused the assembler to flag any identifiers whose length exceeded 1024 characters with an assembly-time error. With this patch, such identifiers are now accepted.
Patch 417.00 OSF440-366	**Patch:** Fixes a problem with floppy driver **State:** Existing This patch fixes a problem with the floppy driver that causes data corruption.
Patch 419.00 OSF440-368	**Patch:** Updates FORE ATM (lfa) driver to Rev. V1.0.17 **State:** Supersedes patches OSF440-078 (72.00), OSF440-198 (251.00) This patch corrects the following: • Updates the FORE ATM (lfa) driver to Revision V1.0.14. • Updates the lfa ATM driver to V1.0.16 and fixes the following two ATM driver problems: – Fixes a soft hang that can occur when running NFS over ATM. – Allows the ATM subsyst. • Updates the lfa ATM device driver to V1.0.17 and adds some enhancements as well as a fix for a kernel memory fault seen when either shutting down or restarting the device driver.
Patch 420.00 OSF440-369	**Patch:** quotactl prototype is now POSIX compliant **State:** Supersedes patch OSF440-137 (111.00) This patch corrects the following: • Fixes a problem where the system can panic with a "kernel memory fault" in dqget. • Fixes a problem where the system can panic with a "kernel memory fault" in dqget.
Patch 421.00 OSF440-370A	**Patch:** Security (SSRT0642U) **State:** Supersedes patches OSF440-149A (123.00), OSF440-251A (287.00), OSF440-301A (364.00) This patch corrects the following: • Fixes a problem of libsecurity producing a core file when handling error conditions. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. • Corrects a problem of the rsh command displaying a warning message instead of the rsh command output when C2 security is configured. • Fixes a problem with logins in a DCE/C2 environment. You could encounter an error "Bad priority setting" if there is a u_priority setting used in /etc/auth/system/default file.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 422.00 OSF440-371	**Patch:** Fixes problems with the mv command **State:** Existing This patch fixes the following problems with the mv command: • An invalid error message when attempting to move files in which the source name is the same as the destination name. • When using mv -i to rename a symlink pointing to a file on a different filesystem owned by a different user, it results in the prompt: Ownership of y will change. Continue? • When moving a file from one filesystem to another, the mv command will copy the file rather than using the rename() system call. This can result in file loss.
Patch 427.00 OSF440-377	**Patch:** Fixes invalid nfscast: select message **State:** Supersedes patch OSF440-024 (22.00) This patch corrects the following: • Fixes a problem in which the automount daemon hangs when invoked by the rsh command. • Prevents the message "nfscast: select: Invalid argument" message from appearing in the daemon.log when the server is not available. It also changes the "trymany: servers not responding: RPC: Unable to receive" message to an informational vs. error message.
Patch 431.00 OSF440-381	**Patch:** Fixes limitation problem for fgrep and egrep **State:** Supersedes patch OSF440-378 (428.00) This patch corrects the following: • Corrects a problem with the fgrep command. When it is used with the -s flag, all output is suppressed. • Fixes a limitation problem with the grep and fgrep commands. If the line length is too long, grep displays a "wordlist too large" error message and fgrep displays "input too long" error message.
Patch 434.00 OSF440-384	**Patch:** file cmd fails to show filenames starting with period **State:** Existing This patch fixes a problem with the find command. Find fails to show filenames that start with a period.
Patch 435.00 OSF440-385A	**Patch:** Adds missing prototype for stime function **State:** Existing This patch adds the missing prototype for the stime() function to <sys/time.h>, allowing C++ programs and other software to properly resolve it.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 436.00 OSF440-386	**Patch:** Fixes for ITPSA driver **State:** Supersedes patches OSF440-062 (56.00), OSF440-119 (95.00), OSF440-129 (103.00), OSF440-072 (151.00), OSF440–235 (274.00) This patch corrects the following: • Fixes a problem in which a system with a KZPCA host bus adapter may hang when the SCSI bus is reset. • Excessive I/O command timeouts when using KZPCM on CLIPPERs causing disk I/O to be retried and fatal tape I/O errors. Additionally the ITPSA driver now supports the KZPCM, 8951U, and 8952U adapters. Support has also been added to identify hardware in the event log. • Fixes the following problems related to the ITPSA driver that supports the KZPCM adapter: – A panic, machine check, or hang can occur when aborting an I/O due to a command timeout or aborting an application program with pending I/Os. – Errors can occur while the system is processing a SCSI bus or SCSI bus device reset request that is issued from the class driver. – On the 8951U and 8952U adapters, SCSI bus resets are lost when these adapters are connected to single-ended drives. – A panic can occur during boot when lockmode is set to 4. • Fixes a problem with the ITPSA driver for KZPCM and KZPCA devices, which resulted in a synchronization problem, causing the SCSI bus to hang. • Fixes the following ITPSA driver problems: – The chip interrupt register fields in error log are incorrect. – Lessens the opportunity of aborts being issued for an already completed I/O. – A kernel memory fault panic caused by a SWS data structure being released twice. – A simple lock timeout panic. It was possible for a bus reset to be generated before the previous bus reset was processed, causing excessive processing within the ISR. – The driver negotiated for ULTRA2 speed when it was attached to a single-ended bus. – The system will panic in itpsa_allocReq() on boot when lockmode=4 is set.
Patch 437.00 OSF440-387	**Patch:** Fix for restore command **State:** New This patch fixes a problem in which the restore command can fail with the following error: Cannot malloc space for property list

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 439.00 OSF440-391	**Patch:** Fix for dbx **State:** Supersedes patch OSF440-101 (78.00) This patch corrects the following dbx problems: • Fixes a problem in viewing a variable subrange parameter from a Pascal module while using dbx. • Dbx stack trace is incomplete. • Assignment to a variable would fail after viewing a non-local symbol. • The use of vfork would raise a signal 66.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 440.00 OSF440-392	**Patch:** Fixes a cpio hanging problem in Japanese locales **State:** Supersedes patches OSF440-017 (15.00), OSF440-026 (23.00), OSF440-027 (24.00), OSF440-028 (25.00), OSF440-146 (120.00), OSF440-055 (142.00), OSF440-066 (145.00), OSF440-077 (156.00)OSF440-096 (175.00), OSF440-318 (376.00), OSF440-359 (410.00) This patch corrects the following: • Fixes a problem with /usr/bin/ksh and the named-pipe (FIFO) communication that is used by applications. • Corrects a problem that was causing ksh to core dump in vi editing mode. ksh was core dumping intermittently when using "." to repeat a command. • ksh does a segmentation fault and core dumps when displaying a here-document. • Fixes problems in ksh, file, tail, nawk, awk, and pax: – Unexpected logouts and terminal hangups occur when using the /bin/su command and /bin/ksh as a login shell. – The file command gives incorrect output concerning WAV audio files. – The tail command gives erroneous output when used with both the -n and -r flags. – The maximum number of fields per record was changed from 99 to 199 for the awk command. – The tar/pax program did not always read the last tape record of an archive. This caused confusion for scripts that were reading a series of archives on the no-rewind device. • Fixes a problem in ksh which required two SIGTERM signals to be sent to the process when it exec'ed. • Corrects a problem that may cause ksh to coredump when displaying a large here-document in a ksh script. • Fixes a problem that caused incorrect file dates to be restored when pax was used to copy files. The problem occurred in the following cases: – If the file was a nonempty directory. – If the file was the target of another symbolic link. • Fixes a core dump from ksh. • Fixes a problem with the Korn shell where data loss occurs when commands are piped together. • Fixes a problem in ksh in which a space after the -p switch would cause the command to fail. • Fixes a problem in ksh. When the current working directory is / and the command cd .. is entered, the following error message is displayed: ksh: ..: bad directory • Fixes a cpio hanging problem in the Japanese locales.
Patch 443.00 OSF440-395	**Patch:** Danish locale now uses all lowercase month names **State:** New This patch updates the Danish (da_DK.ISO8859-1) locale to use all lowercase month names.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 444.00 OSF440-396	**Patch:** Fixes sort problem when running in Japanese locale **State:** Supersedes patch OSF440-051 (45.00), OSF440-283 (316.00) This patch corrects the following: • Fixes a problem in which sort -i a_file >b_file aborts with message "A line of the input file contains more than 20480 characters" when LANG = da_DK.ISO8859-1. • Fixes a problem in which sort command aborts with message "A line of the input file contains more than 20480 characters" when running in a Japanese locale. • Fixes a problem that sometimes occurs when sorting large data files in a multibyte locales like Japanese.
Patch 447.00 OSF440-399	**Patch:** Fixes a problem with the psiop driver **State:** Supersedes patch OSF440-163 (225.00) This patch corrects the following: • Fixes a panic when using the scu command. When formatting a floppy using the scu command the system panics with the following error message: System Uncorrectable Machine Check 660 (retry set) • Fixes a problem with the psiop driver that causes it to fail when vdump is used. The following error is displayed: vdump : unable to write to device
Patch 448.00 OSF440-400	**Patch:** btcreate does not wait long enough between vdumps **State:** Supersedes patches OSF440-285 (318.00), OSF440-171 (231.00), OSF440-343 (394.00) This patch corrects the following: • Fixes a problem with the btcreate command where it does not pass the full pathname to newfs. • Corrects a problem in the btextract script which could result in the failure of the script due to a problem in the use of the grep utility in the script. • Fixes a problem with the btcreate command where default restore fails if disklabel is different. • Fixes a problem with btcreate not waiting long enough for the next tape to be loaded with some media changers.
Patch 449.00 OSF440-401	**Patch:** Fix for C shell problem **State:** Supersedes patches OSF440-114 (90.00), OSF440-009 (168.00), OSF440-226 (269.00) This patch corrects the following: • Corrects how the C shell handles 2-byte characters when running in the Japanese SJIS locale. • Corrects the printing of Japanese SJIS strings that are assigned to shell variables in the C shell (csh). • Fixes a problem in the C shell (csh) in which a segmentation fault will occur when the user defines an environmental variable which exceeds the 2048 character limitation. This limit has been lengthened to 8192 characters. • Fixes a C shell problem where multibyte characters may not be displayed properly inside quotes.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 450.00 OSF440-402	**Patch:** Fixes several DEC C compiler problems **State:** Supersedes patches OSF440-134 (108.00), OSF440-293 (325.00) This patch corrects the following: • A compiler problem that allowed the generation of EV67 (CIX) instructions to be generated when using the -arch ev6 switch. • A compile time performance problem with a very large (1.6 MB) array initialization. • An optimization problem that caused incorrect output when using a signed char in a strcpy-like routine, if compiled using -O4 or higher. • A compile-time error for a source line such as a = strcpy(b,c) + 7. • An optimizer problem that caused an unintended sign-extension in the Perl program. This caused an "op/pack" failure in test 9. • A compiler crash when compiling Xemacs 21.1.4 with -O4. • An optimizer problem in loop unrolling that suppressed intermediate updates to induction variables under certain conditions. • A particular short parameter assignment caused incorrect run-time result. • An assignment of type k = (char)(l >> 8) was not sign-extended. • An optimizer problem that produced incorrect code when certain bounds checking within a loop was moved outside the loop. • An optimizer problem that caused the wrong result when compiled at -O2, under certain conditions. • A virtual memory exhausted error when compiling the Open Source encryption library OpenSSL. • A compiler crash under certain conditions that produces an Assertion failure: Non-Arithmetic Data Type error.
Patch 451.00 OSF440-403	**Patch:** Memory channel driver may result in panics with rm **State:** Supersedes patch OSF440-118 (94.00) This patch corrects the following: • Fixes a problem where an MC1 or 1.5 will not configure with an ev6 8x00. It also improves error handling with MC 2 in a Virtual Hub. • Fixes a problem in the memory channel driver which could result in panics with rm - inconsistent local spinlock structures being logged.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 452.00 OSF440-404	**Patch:** Fixes for vrestore problems **State:** Supersedes patches OSF440-048 (42.00), OSF440-237 (276.00) This patch corrects the following: • The command was slow to complete when a partial restore operation was requested. • The command failed to ignore extended attribute records for the files which were not requested for a vrestore operation. • Fixes problem with vrestore where vrestore fails to restore certain files and directories having ACLs from a compressed vdump saveset, reporting: vrestore: error setting extended attributes 22 • A previous patch caused incomplete restores. • A warning message is displayed when the path for the first file in a group of hardlinks is created without using original protection codes and property lists. • A warning message is displayed and vrestore aborts if it fails to malloc space for a property list. • A message which had been inserted at the end of the message file had the wrong message category (could cause messaging confusion). • An uninitialized variable in the code that restores property lists could cause malloc failures, memory faults, "error setting extended attributes", and infinite loops using the -l option. • Corrupted property list information could cause an infinite loop.
Patch 454.00 OSF440-406	**Patch:** Incorrect results when using disk statistics tools **State:** Supersedes patches OSF440-005 (44.00), OSF440-224 (267.00), OSF440-238 (277.00), OSF440-255 (290.00), OSF440-319 (333.00), OSF440-298 (363.00), OSF440-308 (367.00) This patch corrects the following: • Fixes a kmf problem in bucket 2 (64 byte bucket) when the type of SCSI device dynamically changes. • Corrects a problem in which the wrong status could be returned when using a tape device. • Increases the performance of random I/O on the HSG80 disk controller. • Fixes a problem in which the system can panic with a kernel memory fault. • Fixes problems with: – Continuous resets when an I/O command is causing the resets – Read capacity recovery failure – Bad block replacement (BBR) processing – Fixes a problem where programs that read, analyze and monitor disk statistics (such as collect) will occasionally display incorrect results. – Fixes a problem in which the system can panic with a kernel memory fault during an installation with an HSZ70 or HSZ80 connected to the system. – Fixes a problem when the type of SCSI device dynamically changes, which can result in a kernel memory fault or memory corruption panic.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 OSF440-408	**Patch:** Security (SSRT0563U) **State:** Supersedes patches OSF440-011 (9.00), OSF440-012 (10.00), OSF440-015 (13.00), OSF440-003 (27.00), OSF440-032 (30.00), OSF440-061 (55.00), OSF440-120 (96.00), OSF440-123 (99.00), OSF440-128 (102.00), OSF440-132 (106.00), OSF440-133 (107.00), OSF440-136 (110.00), OSF440-142 (116.00), OSF440-143 (117.00), OSF440-148 (122.00), OSF440-152 (126.00), OSF440-155 (129.00), OSF440-039 (141.00), OSF440-067 (146.00), OSF440-081 (160.00), OSF440-085 (164.00), OSF440-095 (174.00), OSF440-033A (31.00), OSF440-099 (178.00), OSF440-104A (81.00), OSF440-138 (112.00), OSF440-164 (134.00), OSF440-164 (134.00), OSF440-158 (224.00), OSF440-170 (230.00), OSF440-180 (238.00), OSF440-182 (239.00), OSF440-187 (244.00), OSF440-194 (248.00), OSF440-204 (255.00), OSF440-206 (257.00), OSF440-209 (259.00), OSF440-221 (265.00), OSF440-227 (270.00), OSF440-256 (291.00), OSF440-259 (294.00), OSF440-268 (303.00), OSF440-272 (307.00), OSF440-276 (310.00), OSF440-278 (312.00), OSF440-284 (317.00), OSF440-144 (118.00), OSF440-036 (33.00), OSF440-056 (49.00), OSF440-057 (50.00), OSF440-058 (51.00), OSF440-059 (52.00), OSF440-112 (88.00), OSF440-125 (100.00), OSF440-141 (115.00), OSF440-147 (121.00), OSF440-060A (54.00), OSF440-082 (161.00), OSF440-305 (331.00), OSF440-166 (227.00), OSF440-174 (234.00), OSF440-208 (258.00), OSF440-213 (261.00), OSF440-220 (264.00), OSF440-244 (280.00), OSF440-257 (292.00), OSF440-265 (300.00), OSF440-289 (321.00), OSF440-097A (176.00), OSF440-303 (329.00), OSF440-168A (229.00), OSF440-107 (83.00), OSF440-191 (246.00), OSF440-159 (131.00), OSF440-088 (73.00), OSF440-065 (58.00), OSF440-207 (180.00), OSF440-239 (210.00), OSF440-253 (288.00), OSF440-269 (304.00), OSF440-288 (320.00), OSF440-294 (326.00), OSF440-018 (16.00), OSF440-157 (130.00), OSF440-314 (332.00), OSF440-073 (152.00), OSF440-219 (263.00), OSF440-116 (92.00), OSF440-070 (149.00), OSF440-071 (150.00), OSF440-216 (181.00), OSF440-196 (250.00), OSF440-240 (278.00), OSF440-270 (305.00), OSF440-110 (86.00), OSF440-292 (324.00), OSF440-160 (132.00), OSF440-200 (360.00), OSF440-297 (362.00), OSF440-302 (365.00), OSF440-307 (366.00), OSF440-309 (368.00), OSF440-310 (369.00), OSF440-311 (370.00), OSF440-312 (371.00), OSF440-313 (372.00), OSF440-317 (375.00), OSF440-320 (377.00), OSF440-322 (379.00), OSF440-324 (380.00), OSF440-328 (382.00), OSF440-335 (388.00), OSF440-337 (389.00), OSF440-340 (391.00), OSF440-341 (392.00), OSF440-342 (393.00), OSF440-346 (397.00), OSF440-347 (398.00), OSF440-348 (399.00), OSF440-352 (403.00), OSF440-353 (404.00), OSF440-360 (411.00), OSF440-361 (412.00), OSF440-362 (413.00), OSF440-363 (414.00), OSF440-367 (418.00), OSF440-372 (423.00), OSF440-373 (424.00), OSF440-374 (425.00), OSF440-375 (426.00), OSF440-379 (429.00), OSF440-380 (430.00), OSF440-382 (432.00), OSF440-383 (433.00), OSF440-393 (441.00), OSF440-394 (442.00), OSF440-397 (445.00), OSF440-398 (446.00), OSF440-405 (453.00), OSF440-407 (455.00), OSF440-414 (459.00), OSF440-415 (460.00), OSF440-417 (462.00), OSF440-295 (327.00), OSF440-250 (286.00), OSF440-331 (385.00), OSF440-419 (464.00), OSF440-418 (463.00), OSF440-364 (415.00)

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	This patch corrects the following: • Fixes a problem where process accounting data was not written to the accounting file when it was on an NFS-mounted file system. • Corrects a "simple_lock: time limit exceeded" panic in softclock_scan(). • Fixes a kernel memory fault from socket code. The kernel memory fault results from failing to get a lock on a list of threads that have requested resources on a socket. • Corrects a problem where a signal is delivered, but not responded to, by the target process. • Fixes a panic of "get_color_bucket: empty buckets" when the sysconfig attribute "private-cache-percent" is non-zero. • A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability. • Fixes a problem with the mount command where it sometimes kills other processes. • Fixes a problem where process accounting data was not written to the accounting file when the accounting file was on an NFS-mounted file system. • Fixes problems with loadable drivers indicated by a maximum device number, lack of device number 0, or failure to reconfigure or reload a driver.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes a problem in which mount would incorrectly fall back to Version 2 after certain errors had been encountered using Version 3. • Fixes an nfs/ufs/vm deadlock. While serving a client, the system running ASE/DT as an NFS server can hang with deadlock. • Fixes a problem in which the system may panic with the error message "kernel memory fault". • Fixes several KZPCC RAID controller problems which in turn provides full support of the product. • Fixes a problem where applications using the fcntl() system calls may appear to hang. • Fixes "simple_lock: time limit exceeded" panics. • Fixes two problems: fork can fail to obtain swap space and the resource limitation on core files does not work as documented. • Fixes a problem where the system can panic with the following console message: bs_bf_htop: invalid handle \n N1 = 0 • Fixes a system pause seen when doing a lot of I/O to UFS filesystems. • Fixes a problem that causes system panics when thread_swappable is called with the current_thread as the target thread, when the thread is about to be swapped out. • This work provides functionality to allow detecting unlinked referenced files. • Fixes a problem with the map entry indexing scheme that results in the following panic: pmap_release_page: page not found • Fixes a problem in which certain invalid kernel address ranges may get ignored. This can result in invalid kernel memory accesses to be left unnoticed. • Fixes a problem that causes the Tru64 UNIX Version 5.0 update install procedure to exit with core dumps and /sbin/loader failures on a system. • Fixes a problem in the module core() that can cause a panic with the message: vrele: bad ref count • Fixes two separate problems: – A panic in the kernel with the following error message: simple_lock: time limit exceeded – A panic occurs when booting kernel interactively and setting the memlimit. The panic error message is as follows: kernel memory fault • Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash. • Removes a Granularity Hint Regions (also called GH chunks) restriction which may be encountered on AlphaServer DS20 and ES40 systems running the Tru64 UNIX V4.0F release. This restriction can reduce performance for certain database applications. • Fixes several problems associated with Controller Reset (hard-error recovery) for the KZPCC backplane RAID controller.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes a system hang condition. All NFS-related services may deadlock. • Fixes the database application core dumps when using truss/trace tools by remembering that COW has been set up on a shared pte and processes it correctly when a subsequent write access is made to the page. • Fixes a data corruption problem that can occur when mapping to private regions. • Fixes a problem where AS1200 systems with more than three pairs of memory displays the following warning message on the console during boot: pmap_get_align: Unaligned memory hole found... Please reset the system to clear any previous memlimit • Fixes a kernel memory fault caused when a network application walked an inpq array. • Fixes a problem in which signals can be lost in multithreaded applications. • Fixes a problem that only occurs if real-time preemption is enabled and SMP test suites are run. • Fixes a problem that could result in a incorrect scheduling of threads when they were dispatched from the idle state. • Fixes a problem with virtual memory. When running the Oracle database, Oracle can not detach from a shared memory segment. • Fixes single-step support in a debugger, such as Ladebug, for instructions that trap or fault. • Fixes an incorrect calculation for memory-usage-by-type when kmem_debug is set. • Fixes a simple_lock: hierarchy violation in sigq_abort() when lockmode is set to 4. • Fixes a system panic on multi-process systems (approximately 12 CPUs) with large memory (128GB). The system can panic with: panic: lock time on vm_page_free_lock • Fixes a problem in which unmounting an NFS mounted directory can cause a user process to coredump. • Fixes a problem where partitioned Turbolasers return incorrect CPU data for CPUs that are not in the partition. • Corrects a problem that was causing degraded performance of the WAN Support for Tru64 UNIX layered product. • Under certain conditions, when using Asynchronous I/O, NULL pointer can be dereferenced in aio_unwire(), causing a kernel memory fault panic. This fix eliminates this possibility. • Fixes a problem where ubc_msync() may not flush out all the pages in the requested range. • Fixes var adm messages from truncation on larger configurations by raising the default size (4096) of msgbuf_size to 8192. • Fixes a problem where systems with the DUV40FAS0002-19991116 patch kit installed would run low on kernel memory after process accounting had been running for a while.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Corrects a problem where a mount(8) command failure caused the operating system to crash. Instead, the failure will now only cause the AdvFS filesystem domain to shut down. • Fixes a problem on systems using the AdvFS filesystem, where the system can panic with the following panic string: del_clean_mcell_list: no primary xtnt record • Fixes an AdvFS domain panic that occurs with the following message on the console: load_x_cache: bad status from bs_refpg of sbm • Fixes a problem with AdvFS that will cause the system to panic with "kernel memory fault" in audit_rec_build(). • Fixes a problem where the statfs system call was reporting incorrect block usage on AdvFS filesets. As a side effect of this problem, the sendmail utility may sleep needlessly (waiting for space to become available). • Provides the following fixes and enhancements to AdvFS: – AdvFS volumes were not setting the default I/O byte transfer size to the preferred size reported by the disk drives. – AdvFS chvol read and write transfer size range was increased. – The read-ahead algorithm was modified to improve performance under certain conditions. • Fixes the problem where the system panics if AdvFS detects an inconsistency in the free list of mcells that is kept on a per-volume basis in an AdvFS domain. The panic string seen with this panic is as follows: alloc_mcell: bad mcell free list • Fixes a problem where update takes too long to sync mmap files when using an AdvFS file system. • Fixes the following two problems in AdvFS: – When a “log half full” or “log full” problem occurs, an entire system will panic. – The error message "ftx_bfdmn_recovery:bad record size\n N1 = 1" is received when the wordCnt, as returned by lgr_read, is not enough to hold the ftxDoneLRT record that precedes each log record in a log page. • Corrects a problem where a "can't clear a bit twice" panic occurs after an unanticipated system crash and an improperly handled AdvFS recovery operation. • Corrects a problem in AdvFS that causes single-CPU systems to hang and causes multiple-CPU systems to panic with a "simple lock time limit exceeded" error specifying lock class name BfAccessTblMutex. • Corrects a problem in AdvFS where unmounting a domain that is already in a panicked state could result in the following system panic message: log_flush_sync: pinpg error\n N1 = 5

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes a problem in AdvFS. AdvFS may skip filesystem recovery after aborted domain activation. • Corrects a kernel memory fault that occurs when entering the mount -o dual command. Abbreviated stack: 9 _XentMM() 10 bs_bfdmn_sweep() 11 bs_bfdmn_activate() 12 bs_bfdmn_tbl_activate() 13 bs_bfset_activate_int() 14 bs_bfset_activate() 15 advfs_mountfs() • Fixes a problem that may cause panics to occur when msfs_getpage() receives an error return from fs_write_add_stg() when attempting to write to an AdvFS domain that is out of disk space. • Fixes a problem in AdvFS. A fileset is busy when attempting to unmount giving an EBUSY error even though the fileset has no open files. • ASE/Disaster Tolerance systems hang when a kernel vnode reclaim flushes a vnode's modified data to disk and ASE/DT is currently suspending I/O requests. • Fixes a problem with making a msfs_putpage() call. The length argument may get its upper bits truncated, which will result in an incorrect length calculation. • Fixes a problem in the AdvFS system. A panic occurs with the following error message: lock_read: hierarchy violation • Fixes a situation in which a slight memory leak can occur when recovering Advfs domains with mount. • Fixes a problem where a single CPU system using AdvFS can hang in cleanup_closed_list(). • Corrects AdvFS problems involving clone filesets. The statfs syscall (used by df) was incorrectly returning zero blocks USED for clones. The read-ahead code was incorrectly passing up opportunities to do read-ahead on clone filesets, resulting in a large performance penalty. • Corrects two problems in AdvFS property list handling: – Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf). – The get_proplist_entry function (used to disassemble the property list buffer returned by the "getproplist" system call) returned incorrect name length on property list names longer than 127 characters. • Fixes a problem with soclose() that caused permanent looping on exit while aborting pending connections at a TCP/IP listener socket. • Fixes a problem with soclose() that caused permanent looping on exit while aborting pending connections at a TCP/IP listener socket. • When configuring the AlphaServer ES40, the ISA devices IDE and USB are not configured if a combo card is installed. • The system panics with a kernel memory fault when installing on a AlphaServer DS20.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes the following Compaq AlphaServer problems: – On the ES40 and DS20, nonfatal 680 environment machine checks are being logged as fatal/noncorrectable errors. – On the DS20, a fix has been made to the handling of power supply, temperature, and fan events so that they are reported correctly. – Provides support for the Compaq AlphaServer DS20E. • Allows the com1_environment variables to be stored in NVRAM. On a DS10 platform, resetting console baud rate to anything other than the rate it was running, a system panic occurs at boot. • Fixes various problems with the driver support for the Powerstorm 4D10T (ELSA Gloria Synergy) graphics board. • Provides the driver support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA) (also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB). • Adds additional error detection to the FC driver. • This patch updates the emx Fiber Channel driver to revision 1.12, adds support for the KGPSA-CA adapter, and also fixes the following problems: – In an ASE environment, the driver was not appropriately restoring the link state after a LIP, which typically occurs when the Fiber Channel cable has been unplugged. – When connected to the new Pleiades II switches, the switch ports would consume target IDs on the adapter's SCSCI bus. – A kernel memory fault in routine emx_handle_els_request. – A system hang at boot up caused by infinitely trying to probe the Fiber Channel link. • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, the graphics were not reset to console mode (the blue screen) when the halt button was pressed. • Fixes several KZPCC RAID controller problems which in turn provides full support of the product. • Updates the emx Fiber Channel driver to Revision 1.17, correcting the following problems: – If connected to a switch that is part of a cascaded set of switches and is not the primary switch in the fabric, the host will never complete link initialization. – Occasionally, the link fails to initialize on the KGPSA-CA at boot. – If the cable connection between the switch and KGPSA-CA was unplugged and then replugged, the KGPSA-CA would fail to properly initialize the link and all FC connections would be terminated until the next system reboot. – Corrects some boot messages indicating mailbox command failures. • Fixes a kernel memory fault caused by a streams SMP race condition.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes the following Universal Serial Bus (USB) problems: – The USB mouse no longer functions after resetting the Xserver. – System panics may occur in error handling after USB device fails a request. – The USB device may not deconfigure properly when unplugged from the bus. – Problems that will prevent some USB devices from being configured at boot time. – A key on a USB keyboard will continue to repeat after being unplugged. – USB keyboards may transmit the incorrect keycode for several keys. • Fixes a system hang in which there is a large number of pending ioctl's on the streams queue. • Fixes a panic in AdvFS which can have the following error messages: panic (cpu 1): bs_cow_pg: pin clone err panic (cpu 1): bs_cow_pg: cannot get blkMap • Fixes a kernel memory fault caused by a mishandling of multicast addresses on the FDDI interface. • Fixes a problem most frequently encountered by the ppp daemon /usr/sbin/pppd when the ppp connection is terminated. When run in debug mode, an exiting pppd will log a message similar to the following when the error is encountered: >> May 25 12:29:17 dragon pppd[2525]: ioctl(SIOCDIFADDR): Invalid argument • Fixes a kernel memory fault and an SMP race condition with the AltaVista Firewall 98 server on a multi-CPU system. • Fixes a problem when a default IP address and a cluster virtual IP address are interchanged after a network restart. The default interface address is used by all outgoing traffic and the alias address is only usable for the incoming packets. • Fixes a problem in which the system may panic with the error message "tcp_output REXMT". • Fixes a problem where RCP commands issued from a Sun Solaris system to Compaq Tru64 UNIX may sometimes fail incorrectly with the error message "Connection reset by peer". • Fixes a TCP performance problem if the TCP window scale option is turned off when using the HIPPI interface. • Fixes a system panic: tcphdr too big • Consists of changes necessary for the AltaVista Firewall 98 to pass ICSA certification. • Fixes a problem with packetfilter applications that use IP packets greater than 8K. • This patch involves virtual mac addressing.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes a problem that caused AdvFS to incorrectly calculate metadata file size for files greater than 4 GB resulting in corruption on read and stat syscalls. • Fixes a bug such that when fuser -k is issued on a dismounted NFS mount point in which some process is running, a hang will occur. • Fixes a problem in which an invalid error status is returned from the remove_entry system call. • Fixes a problem in which the interaction between NFS file systems and Smoothsync causes procprod to read stale data. • Fixes a kernel memory fault when accessing the vm_map_index hash table. • Fixes a simple_lock time limit exceeded panic due to an SMP race condition in namecache. • Fixes a problem that causes corruption in the floating point registers whereby the flag fields nxm_fp_owned are overwritten with 0s. • Fixes a problem in AdvFS. The system panics with a kernel memory fault. • Fixes a problem in AdvFS. A system panic occured with the following error message: panic: del_dealloc_stg(): cant ref bmt page • Fixes a kernel memory fault in VMAC code if_addnewaddr(). • Fixes a system hang that could last up to a few minutes with large files when performing synchronous IO requests. • Fixes a system panic with the panic string: psig: catch not set • Corrects a kernel memory fault caused by rw3vp_cache passing a bad address to _OtsZero(). • Corrects a problem in which the perrmask register on Tsunami systems can be overwritten. • Fixes a problem where the output of a ps command, the PAGEIN column reports 0 for all processes. • Fixes a problem in which an application can hang because of an undelivered signal.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes a problem in Advfs. A panic occurs with the following error message: lock_read: hierarchy violation • Fixes a problem where the system appears to hang. A child process is holding a lock too long and preventing other processes from doing work. • Fixes a problem where, if the size of the message queue was increased, writers to the queue that were blocked would not wake up for processing. • Fixes a problem in which the POSIX interval timer is not resilent to clock slowdown caused either by NTP or by a backwards change of the clock. • Fixes a system panic that was seen on large configurations under a heavy load situation. • Provides the latest driver for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card and the latest graphics driver for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA). • Fixes a problem in AdvFS where putpage_lk/pg_busy deadlock causes hangs in the system. • Fixes several panics on systems with holes in memory. The error messages are listed below: panic: put_free_ptepage: invalid pvh state panic: kernel memory fault trap: invalid memory read access from kernel mode panic: not wired simple_lock: hierarchy violation • Adds a fix to VMAC functionality when used with NETrain. • Fixes a problem where the following can occur during a system panic: – System calls interrupts – mpsleep() returns an EINTR error when the panicstr is non-NULL – An indefinite looping at a very high priority • Fixes AdvFS inconsistent quota problems and errors similar to the following appearing on the console: vmunix: chk_bf_quota: group quota underflow • Fixes a problem with verify. When verify is run on a brand new domain, NFS warnings are displayed even though no NFS related activity is being done. • Corrects a problem with the incorrect ordering of network interfaces which was resulting in network partitions. • Fixes a "lock_terminate: lock held" panic when deleting a process group. • Fixes an "unaligned kernel space access from kernel mode" panic when doing a malloc from kmembucket 26, 896 byte bucket. The faulting virtual address will be the lock signature for thread_deallocate(). • Fixes a kernel memory fault in u_anon_faultpage() when it accesses the backing object for the anonymous page.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes a problem where a root user was not allowed to check file access on behalf of a user without completely becoming the user. The functionality is needed by the ASU (Advanced Server for UNIX) product. • Fixes a panic in in_pcbfree() associated with ASE service failover. • Fixes a file system panic which has the following error message: syscall: complex lock owned • Fixes an AdvFS problem which caused the system to crash with a kernel memory fault. • Includes UFS delayed metadata mount option that fixes metadata intensive application performance. • Fixes a kernel memory fault seen under certain conditions when setting a thread's priority. • Fixes a race condition in the UBC code where a lookup is done on a page being invalidated (freed). • Fixes a race condition involving signals and threads that only happens on multiprocessor systems. • Fixes a problem with a kernel memory fault in AdvFS. • Fixes a problem where the operating system only looks in slot 0 for the primary CPU. • Corrects a KZPCC lock problem that is seen when a kernel is run with lockmode set to four. This patch also resolves a timing issue which prohibited the KZPCC product from being seen during boot on EV67 platforms. • Fixes a kernel memory fault caused by either one of the following conditions: – On EV6 platforms, when the debugger is used to view the OT_DEVMAP object mapping memory in I/O space that is mapped to a user process. – When routine pmap_coproc_exit_notify() modifies the pmaps' coproc_tbi function to be 0, a null pointer, while it is being checked by routine pmap_remove_all(). • Fixes a problem in which operations on NFS files can hang indefinitely. • Updates the emx Fiber Channel driver to revision 1.21 which corrects a Data Error that is seen when running with the latest Emulex firmware. This error corrupts data when reading from the disk. • Fixes a problem in which an invalid PCI entry in sysconfigtab can cause the system to be unbootable. • Fixes a problem in which a PCI bridge-based boot device may fail to configure on large I/O systems.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 456.00 continued	• Fixes a problem where genvmunix does not boot on a system with an Atalla AXL200 card installed. • Fixes several problems specific to AlphaServer 1200 and AlphaServer 4100 systems. – The user.log file has the following message: redundant power supply failure – The messages file has the following intermittent messages: ERROR: i2c_read_temp: environmental monitoring error ERROR: i2c_read_fail_reg: environmental monitoring error ERROR: i2c_read_func_reg: environmental monitoring error – Systems were shutting themselves down displaying the following message: System has reached a high temperature condition. Possible problem source: Clogged air filter or high ambient room temperature. • Modification to pci resource management to allow support behind pci bridges for the AXL200 card.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 457.00 OSF440-411A	**Patch:** Addresses performance and scalibility issues **State:** Supersedes patches OSF440-102 (79.00), OSF440-151 (125.00), OSF440-035 (138.00), OSF440-093 (172.00), OSF440-115 (91.00), OSF440-098 (177.00), OSF440-094 (173.00), OSF440-193 (247.00), OSF440-223 (266.00), OSF440-357 (408.00), OSF440-054A (48.00), OSF440-388 (438.00), OSF440-111 (87.00) This patch corrects the following: • Modifies the strftime() function to make the %V format specifier return the correct week. • Fixes a problem of password error messages not being displayed during installation of the security subsystem. • The routines wprintf(), swprint(), and fwprintf() do not handle the S format correctly. Instead of treating the data as logical characters, they treat data as bytes. • Fixes problems with rsh(1), rlogin(1), and rcp(1) if netgroup names are defined with uppercase letters. • Fixes a problem with portmap by allowing RPC select() timeouts to occur when interrupted by signals. • Fixes and enhances the quotacheck and fsck commands. • Fixes a problem in which the fsck utility may be unable to repair a UFS filesystem. • Fixes a problem in which ufs_fsck can get blocked while attempting to flush NFS buffers for a service that has become suspended. • Fixes a problem that was causing the csh globbing function to be extremely slow when accessing file information on NFS, AFS, or VMSTM™ file systems. • Increases the length of the user names for rsh and rexec to allow for NT interoperabilty. • Fixes a problem where gmtime() was erroneously setting the tzname[0] array. • Fixes problems in the DECthreads library for Tru64 UNIX. Included in this patch are changes to support Ladebug enhancements and a bug fix for applications which employ SCS threads of different priorities. • Fixes bugs in the DECthreads library that would affect threaded applications running on Tru64 UNIX V4.0F. The changes are related to synchronous signal processing and thread scheduling. • Addresses performance and scalibility issues for highly contended threaded applications running on EV6 SMP machines.
Patch 458.00 OSF440-412	**Patch:** Security (SSRT0567U, SSRT0590U) **State:** Supersedes patches OSF440-014 (12.00), OSF440-109 (85.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. • Fixes a problem where some crontab jobs would run multiple times in the same minute.
Patch 461.00 OSF440-416	**Patch:** Cursor is displayed incorrectly **State:** New This patch fixes a problem where the cursor is displayed incorrectly when the image plane is set to 1 and the mask plane is set to 0.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 465.00 OSF440CDE-019B	**Patch:** Security (SSRT0617U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 467.00 OSF440CDE-020B	**Patch:** Fix for dtfile tool **State:** New This patch fixes a problem in which dtfile ICDE COSE tool does not work when TMPDIR is defined as /ldata/disk_local/tmp. dtfile returns this error: /ldata/disk_local/tmp/sdtdbcache_AAAaadmma: Cross-device link /ldata/disk_local/tmp/sdtdbcache_BAAaadmma: Cross-device link Floating exception (core dumped)
Patch 468.00 OSF440X11-020B	**Patch:** Static library fix for svn widget **State:** New This patch fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.
Patch 469.00 OSF440X11-025B	**Patch:** Fix for X server interaction with X font server **State:** New This patch fixes various problems with the X font server and with the X server's interaction with X font servers.
Patch 470.00 OSF440X11-025C	**Patch:** Problem with X server interaction **State:** Supersedes patch OSF440X11-003 (63.00) This patch corrects the following: • Fixes a problem where the X font server (xfs) sometimes failed with a segmentation fault when it received an invalid request. • Fixes various problems with the X font server and with the X server's interaction with X font servers.
Patch 471.00 OSF440X11-026B	**Patch:** Core dump when using multibyte-character locale **State:** Supersedes patch OSF440X11-010B (334.00) This patch corrects the following: • Fixes a problem in which ^C fails to work in dtterm when logged in to a 4.0E or 4.0F system using XDMCP. • Prevents a potential core dump from the X11 library when running an input method server for Japanese, Chinese, or Korean.
Patch 473.00 OSF440-370B	**Patch:** Security (SSRT0642U) **State:** Supersedes patches OSF440-149B (203.00), OSF440-251B (338.00), OSF440-301B (472.00) This patch corrects the following: • Fixes a problem of libsecurity producing a core file when handling error conditions. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. • Corrects a problem of the rsh command displaying a warning message instead of the rsh command output when C2 security is configured.

Table 2–2: Summary of Base Operating System Patches (cont.)

Patch 474.00 OSF440-385B	**Patch:** stime function does not compile under C++ **State:** New This patch adds the missing prototype for the stime() function to <sys/time.h>, allowing C++ programs and other software to properly resolve it.
Patch 475.00 OSF440-425	**Patch:** Fixes kernel panic occuring in lockmode 4 **State:** New This patch fixes a kernel panic seen when running Classical IP over the lfa ATM driver. This panic would only occur in lockmode 4. If not in lockmode 4, the symptom would be a CPU hang.
Patch 476.00 OSF440-411B	**Patch:** Performance issues on EV6 SMP machines **State:** Supersedes patch OSF440-054B (71.00) This patch corrects the following: • Fixes problems in the DECthreads library for Tru64 UNIX. Included in this patch are changes to support Ladebug enhancements and a bug fix for applications which employ SCS threads of different priorities. • Addresses performance and scalibility issues for highly contended threaded applications running on EV6 SMP machines.

3

Summary of TruCluster Software Patches

This chapter summarizes the TruCluster software patches included in Patch Kit-0004.

Table 3–1 lists patches that have been updated.

Table 3–2 provides a summary of patches.

Table 3–1: Updated TruCluster Software Patches

Patch IDs	Change Summary
Patches 30.00, 33.00, 34.00, 35.00, 36.00, 37.00, 45.00, 48.00	New
Patches 6.00, 15.00, 40.00	Patch 42.00
Patches 2.00, 9.00, 10.00, 5.00, 13.00, 16.00, 17.00, 14.00, 29.00, 31.00, 38.00, 39.00, 47.00, 21.00, 49.00, 32.00	Patch 43.00
Patch 20.00	Patch 46.00
Patches 22.00, 23.00, 24.00, 25.00, 50.00	Patch 51.00

Table 3–2: Summary of TruCluster Patches

Patch IDs	Abstract
Patch 3.00 TCR160-003	**Patch:** DRD Permissions May Be Lost **State:** Existing This patch fixes a problem where DRD permissions could be lost if a service is modified more than once.
Patch 4.00 TCR160-004	**Patch:** Fix for Kernel Memory Fault On DRD Client Nodes **State:** Existing This patch fixes a kernel memory fault on the DRD client nodes just as or after the DRD server node has initiated MC2 hub failover.
Patch 7.00 TCR160-010	**Patch:** Fix for Reliable Datagram API **State:** Supersedes patch TCR160-001 (1.00) This patch corrects the following: • Reliable Datagram (RDG) messaging support. • RDG: bug fix to the completion queue synchronization protocol.
Patch 8.00 TCR160-011	**Patch:** doconfig may hang when running in TruCluster environment **State:** Existing This patch fixes two problems that could cause doconfig to appear to hang when running in a TruCluster environment.
Patch 12.00 TCR160-018	**Patch:** Fixes problem with Networker displaying characters **State:** Existing This patch corrects a problem with Networker displaying garbage characters following service names. It occurs when the service name is 8 characters or greater.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 26.00 TCR160-032	**Patch:** Fixes rm_update_single_lock_miss panic **State:** Supersedes patches TCR160-017 (11.00), TCR160-027 (19.00) • Fixes a problem where both nodes in a cluster will panic at the same time with a simple_lock timeout panic. • Fixes a kernel memory fault in rm_lock_update_retry(). • Fixes a problem which can cause the following panic: panic (cpu 0): rm_update_single_lock_miss: time limit exceeded
Patch 30.00 TCR160-034	**Patch:** Fix for boot failure on a cluster **State:** New This patch fixes a problem which caused a boot failure on a cluster with a large number of shared SCSI buses.
Patch 33.00 TCR160-037	**Patch:** Fix for drdadmin problems **State:** New This patch fixes various problems with drdadmin to be user friendly.
Patch 34.00 TCR160-038	**Patch:** Fixes a limitation in ase_reconfig_bus **State:** New This patch fixes a limitation in ase_reconfig_bus. Now up to 99 buses can be reconfigured with this command.
Patch 35.00 TCR160-039	**Patch:** LSM disk information not updated in ASE database **State:** New. Supersedes patch TCR160-030 (28.00) This patch corrects the following: • Fixes a problem that would cause an error from awk(1) when modifying an ASE service that contained a large number of LSM volumes. The error would prevent the service from being properly modified. • Fixes a problem where LSM disk information was not properly updated in the ASE database when volumes were removed from a disk service.
Patch 36.00 TCR160-040	**Patch:** Fix for asedirector hang **State:** New This patch fixes a problem that could cause an NFS or Disk Service that has a hyphen (-) in the service name to end up unassigned after a disk failure. A side effect of the problem was that the asedirector would hang after the disk failure was corrected.
Patch 37.00 TCR160-041	**Patch:** clu_ivp does not recognize Emulex adapter **State:** New This patch fixes a problem where the Emulex Fibre Channel adapter was not recognized by clu_ivp.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 42.00 TCR160-046	**Patch:** Processes may get referenced several times **State:** Supersedes patches TCR160-008 (6.00), TCR160-023 (15.00), TCR160-044 (40.00) This patch corrects the following: • Fixes a problem in which a cluster node can panic with the panic string "convert_lock: bad lock state". • Corrects a problem in which a failure in the session layer can cause DLM messages to become corrupt resulting in random DLM panic on the receiving member. • Fixes a problem that can cause a TruCluster member to panic during shutdown. • Fixes a bug where sometimes a certain shared sequence number will not be freed after use. It also fixes a problem where certain processes could get referenced several times.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 43.00 TCR160-047A	**Patch:** Fix for asemgr utility **State:** Supersedes patches TCR160-002 (2.00), TCR160-009A (9.00), TCR160-016 (10.00), TCR160-007 (5.00), TCR160-021A (13.00), TCR160-024 (16.00), TCR160-025 (17.00), TCR160-022A (14.00), TCR160-033 (29.00), TCR160-035 (31.00), TCR160-042 (38.00), TCR160-043 (39.00), TCR160-051 (47.00), TCR160-031A (21.00), TCR160-053 (49.00), TCR160-036A (32.00) This patch corrects the following • Fixes two problems in the asedirector: – An ASE command timeout problem encountered by large ASE services. – An incorrect decision made by the asedirector as a result of a failed inquire services command. • This is a performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts. • Fixes a problem where the Host Status Monitor (asehsm) incorrectly reports a network down (HSM_NI_STATUS DOWN) if the counters for the network interface get zeroed. • Fixes an ASE problem where, under certain circumstances, the service scripts could cause the ASE agent to loop during a start or stop service. • Corrects a problem with member add in a large environment. • Corrects a problem with TruCluster Available Server or Production Server cluster in which services have been started with elevated priority and scheduling algorithm. Under significant load this could lead to intermittent network and cluster problems. • Fixes a problem which caused a service not to start when there was a short network failure. This was seen only with long running stop scripts and special network configurations. • Corrects a problem which causes asemgr to core dump when modifying a single drd service to add more than 200 devices. • Fixes a problem that caused aseagent or asehsm to core dump when starting NFS and Disk Services that contain several LSM volumes. • Fixes a problem where the asemgr will hang as it continuously create and kill multiple directors. • Corrects a problem that causes the ASE director to core dump during initialization. • Corrects a problem where modifying a service with a large number of DRDs will fail and a "could not malloc" message is seen in the daemon.log. • Fixes a problem where the MEMBER_STATE variable always is shown as BOOTING instead of RUNNING. After first installing TCR, there is no way to have scripts know the MEMBER_STATE. This problem is cleared on a reboot. • Corrects a problem in which a network cable failure that corrects within 7 seconds of the failure can leave the services in a bad state. • Fixes a problem that caused the asemgr to get a memory fault when adding multiple services in a row. • Fixes a problem with extraneous compiler warnings about strdup() function calls from ASE. • Fixes a problem that caused the asemgr utility to not run when called from a program that is owned by root and has the setuid bit turned on.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 45.00 TCR160-049	**Patch:** UFS device name does not display when using asemgr **State:** New. Supersedes patches TCR160-045 (41.00), TCR160-048 (44.00) This patch corrects the following: • Fixes a problem that caused the setting of the "force unmount" option to be incorrectly displayed by the asemgr utility. • Fixes a problem that caused shell errors if an invalid mount option was specified via the asemgr menu. • Fixes a problem that caused the device name for a Unix File System (UFS) to not be displayed when modifying the "force unmount" option via the asemgr utility.
Patch 46.00 TCR160-050	**Patch:** Fix for panic caused by using Memory Channel API **State:** Supersedes patch TCR160-029 (20.00) This patch corrects the following: • Fixes a hang problem in a cluster when two nodes communicate using the mc-api and a third node, not involved in the calculation, is rebooted. • Fixes a problem that can cause a panic in mcs_wait_cluster_event() when using the Memory Channel API.
Patch 48.00 TCR160-052	**Patch:** Error msg incorrectly logged for cnxmibd **State:** New. Supesedes patch TCR160-028 (27.00) This patch corrects the following: • Fixes a problem that can cause the Cluster MIB daemon (cnxmibd) to core dump in Available Server environments. • Fixes a problem which caused an error message to be logged for the cnxmibd even though no error had occurred.
Patch 51.00 TCR160-047B	**Patch:** asemgr does not run when called by root owned program **State:** Supersedes patches TCR160-009B (22.00), TCR160-021B (23.00), TCR160-022B (24.00), TCR160-031B (25.00), TCR160-036B (50.00) This patch corrects the following: • This is a performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts. • Corrects a problem with member add in a large environment. • Corrects a problem which causes asemgr to core dump when modifying a single drd service to add more than 200 devices. • Fixes a problem that caused aseagent or asehsm to core dump when starting NFS and Disk Services that contain several LSM volumes. • Fixes a problem with extraneous compiler warnings about strdup() function calls from ASE. • Fixes a problem that caused the asemgr utility to not run when called from a program that is owned by root and has the setuid bit turned on.