

# Tru64 UNIX 4.0F and TruCluster 1.6

---

## Patch Summary and Release Notes for Patch Kit-0002

**November 1999**

This manual describes the release notes and contents of Patch Kit-0002. It provides any special instructions for installing individual patches.

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

---

© 1999 Compaq Computer Corporation

COMPAQ, the Compaq logo, and the Digital logo are registered in the U.S. Patent and Trademark Office. The following are trademarks of Digital Equipment Corporation: ALL-IN-1, Alpha AXP, AlphaGeneration, AlphaServer, AltaVista, ATMworks, AXP, Bookreader, CDA, DDIS, DEC, DEC Ada, DECevent, DEC Fortran, DEC FUSE, DECnet, DECstation, DECSsystem, DECTerm, DECUS, DECwindows, DTIF, Massbus, MicroVAX, OpenVMS, POLYCENTER, PrintServer, Q-bus, StorageWorks, Tru64, TruCluster, TURBOchannel, ULTRIX, ULTRIX Mail Connection, ULTRIX Worksystem Software, UNIBUS, VAX, VAXstation, VMS, and XUI. Other product names mentioned herein may be the trademarks of their respective companies.

UNIX is a registered trademark and The Open Group is a trademark of The Open Group in the US and other countries.

---

# Contents

## About This Manual

### 1 Release Notes

1.1	Required Storage Space .....	1-1
1.2	New dupatch Features .....	1-2
1.2.1	dupatch-Based Patch Kits for ASE and TCR Patches .....	1-2
1.2.2	New Cross-Product Patch Dependency Management .....	1-2
1.2.3	Patch Special Instruction Handling by dupatch .....	1-2
1.2.4	Patch Tracking and Documentation Viewing .....	1-2
1.2.5	System Patch Baselining .....	1-2
1.2.6	New Command-Line Interface Switches .....	1-3
1.2.7	Compatibility Between Revisions of dupatch .....	1-3
1.3	Release Note for NCR810 Controller .....	1-3
1.4	Release Notes for Patch 210.00 .....	1-3
1.4.1	PCI To Ethernet/Graphics Combo Adapter .....	1-3
1.4.2	Pleiades II Switches .....	1-4
1.5	Release Notes for Patch 118.00 .....	1-4
1.5.1	I/O Throttling/Smooth Sync .....	1-4
1.5.2	Granularity Hint Regions Restriction Removal .....	1-6
1.5.3	Incorrect Error Message .....	1-8
1.6	Release Notes for Patch 173.00 .....	1-8

### 2 Summary of Base Operating System Patches

### 3 Summary of TruCluster Software Patches

#### Tables

2-1	Updated Base Operating System Patches .....	2-1
2-2	Summary of Base Operating System Patches .....	2-2
3-1	Updated TruCluster Software Patches .....	3-1
3-2	Summary of TruCluster Patches .....	3-1



---

# About This Manual

This manual contains information specific to Patch Kit-0002 for the Tru64 UNIX Version 4.0F operating system and TruCluster 1.6 software products. 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 document called *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 *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](mailto: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

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.

---

## 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-0002.

### 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 ~32.1 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 ~32.4 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 ~296 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

A total of ~105 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 ~33.4 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 ~33.8 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 ~213 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

A total of ~105 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

## 1.2 New dupatch Features

The following sections describe new features of `dupatch`.

### 1.2.1 dupatch-Based Patch Kits for ASE and TCR Patches

Patches for ASE and TCR are now installed, removed, and managed through `dupatch`. The ASE and TCR patch kits have been converted to `dupatch`-based patch kits and distributed in the same patch distribution as the applicable operating system.

The multiproduct support within `dupatch` is most visible when installing or removing patches. `dupatch` will display a list of the products that are on the system and in the patch kit, allowing the user to select one or more products before proceeding with patch selections.

You must load the new patch tools provided in this patch kit. See the *Patch Kit Installation Instructions* for more information.

Since all prior ASE and TCR patches have been installed manually, you must set the system patch baseline. See the *Patch Kit Installation Instructions* for detailed information.

### 1.2.2 New Cross-Product Patch Dependency Management

The `dupatch` utility now manages patch dependencies across the Tru 64 UNIX operating system and TCR patch kits. An example of patch cross-product dependency handling for a system with both Tru64 UNIX 4.0F and TCR 1.6 installed follows:

- If a Tru64 UNIX 4.0F Patch 1.00 is chosen for installation and it depends upon TruCluster 1.6 Patch 17.00, which is not already installed or chosen for installation, the `dupatch` installation precheck will warn you of the dependency and block the installation of the Tru64 UNIX 4.0F Patch 1.00.  
If the patch selections are reversed, `dupatch` will still warn you and block installation of the chosen patch.

### 1.2.3 Patch Special Instruction Handling by dupatch

The format and content of the per-patch special instructions has been revised to make it easier to use. You can view the special instructions are now displayed when patches are removed. The per-patch special instructions through the `dupatch` documentation menu.

### 1.2.4 Patch Tracking and Documentation Viewing

The patch tracking and documentation viewing features within `dupatch` can now be used in multi-user mode by nonroot users. See the *Patch Kit Installation Instructions* for more information.

From the `dupatch` patch tracking menu you can now list the patch kits from which patches installed on your system originated.

### 1.2.5 System Patch Baseline

The system patch baselining feature of `dupatch` has been improved. Phase 4 now reports all missing or unknown system files, regardless of their applicability to the patch kit. This will help you identify the origin of manually changed system files. See the *Patch Kit Installation Instructions* for more information.

## 1.2.6 New Command-Line Interface Switches

The `dupatch` command-line mode contains the following new switches:

- The `-product` switch must be used when you specify the `-install` or `-delete` switches when the target system has more than one installed product that is on the kit (such as Tru64 UNIX Version 4.0F and TCR). This switch allows you to specify the product name that the rest of the patch operations will affect. The `-product` switch must precede the `-patch` switch on the command line. See the *Patch Kit Installation Instructions* for more information.
- A `-nolog` switch has been added to enable you to turn off session logging.
- The `-version` switch is no longer used for delete. Using this switch will cause an error and the help information will be displayed on the screen.

Any error on the command line will cause the help information to be displayed on the screen.

If any mandatory switch is missing when using the command-line interface, the command fails with the appropriate usage message. Once you select the command line interface, `dupatch` will not go into interactive mode. Prompting is no longer mixed with the command-line interface.

## 1.2.7 Compatibility Between Revisions of `dupatch`

The new `dupatch` will work with older revisions of `dupatch`-based patch kits.

The older revisions of `dupatch`, however, revision 15 and lower, do not know how to install, remove, or manage patches from the new style patch kits. Please ensure that you load the new patch installation tools when you receive this patch kit. See the *Patch Kit Installation Instructions* for more information.

## 1.3 Release Note for NCR810 Controller

A disk attached to a NCR810 controller may experience an `ss_perform_timeout` error, from which it will then recover. Compaq is investigating this problem and it will be addressed in a future patch kit release of TRU64 UNIX.

## 1.4 Release Notes for Patch 210.00

This section contains release notes for Patch 210.00.

### 1.4.1 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.

## 1.4.2 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 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`). Please refer to 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.

## 1.5 Release Notes for Patch 118.00

This section contains the release notes for Patch 118.00.

### 1.5.1 I/O Throttling/Smooth Sync

---

#### Note

---

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

---

To enable this functionality, edit `/etc/inittab` to contain the following two lines after the line containing `update`. This enables `smoothsync` on transitions into `multiuser`, and disables `smoothsync` on transitions into `singleuser`.

```
smsync:23:wait:/sbin/sysconfig -r vfs smoothsync-age=30 > /dev/null 2>&1
```

```
smsyncS:Ss:wait:/sbin/sysconfig -r vfs smoothsync-age=0 > /dev/null 2>&1
```

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 `msync2` setting.

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

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

to:

```
/dev/rz12e /mnt/test ufs rw,msync2,throttle 0 2
```

---

**Note:**

---

If you choose not to use `msync2` (which does not affect `mmaped` buffers), just remove the `msync2` option from the previous string.

---

Append to `/etc/sysconfigtab` any tuning changes. See the following 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 in which large numbers of dirty pages are locked on the device queue are minimized.

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.

## 1.5.2 Granularity Hint Regions Restriction Removal

This patch removes a Granularity Hint Regions (also called GH chunks) restriction which may be encountered on AlphaServer 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 Administration*, 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="ffffffc0000430000"
```

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.

---

### 1.5.3 Incorrect Error Message

After installing Patch 118.00 on a AlphaStation 1200 with more than three pairs of memory, the following warning message is displayed on the console during boot:

```
Loading vmunix symbol table ... [1316632 bytes]
  pmap_get_align: Unaligned memory hole found: rpb_cluster[4]:
0xfffffffff800e38
  Please reset the system to clear any previous memlimit
```

This message can be ignored and the system will continue to boot. This problem will be fixed in the next patch kit release.

## 1.6 Release Notes for Patch 173.00

The following release notes provide updated information for the `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 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.

## Summary of Base Operating System Patches

This chapter summarizes the base operating system patches included in Patch Kit-0002.

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 76.00, 77.00, 78.00, 80.00, 82.00, 84.00, 86.00, 89.00, 93.00, 94.00, 98.00, 101.00, 104.00, 105.00, 108.00, 111.00, 114.00, 119.00, 123.00, 124.00, 127.00, 128.00, 131.00, 132.00, 135.00, 136.00, 139.00, 140.00, 144.00, 147.00, 148.00, 153.00, 158.00, 159.00, 162.00, 167.00, 168.00, 169.00, 170.00, 173.00, 177.00, 181.00, 182.00, 183.00, 186.00, 187.00, 188.00, 193.00, 194.00, 195.00, 196.00, 198.00, 203.00, 204.00, 205.00, 206.00, 208.00, 209.00, 210.00	New
Patch 201.00	Superseded by Patch 93.00
Patch 202.00	Superseded by Patch 101.00
Patch 109.00	Superseded by Patch 114.00
Patch 83.00	Superseded by Patch 131.00
Patches 97.00	Superseded by Patch 140.00
Patch 90.00	Superseded by Patch 168.00
Patch 91.00	Superseded by Patch 173.00
Patches 79.00, 125.00, 138.00, 172.00	Superseded by Patch 177.00
Patches 92.00, 149.00, 150.00	Superseded by Patch 181.00
Patch 192.00	Superseded by Patch 187.00
Patches 189.00, 190.00, 191.00	Superseded by Patch 193.00
Patches 113.00, 207.00	Superseded by Patch 208.00
Patch 12.00	Superseded by Patch 85.00
Patch 48.00	Superseded by Patch 87.00
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	Superseded by Patch 118.00
Patches 56.00, 95.00, 103.00	Superseded by Patch 151.00
Patches 16.00, 130.00	Superseded by Patch 152.00
Patch 57.00	Superseded by Patch 154.00
Patch 39.00	Superseded by Patch 165.00
Patches 15.00, 23.00, 24.00, 25.00, 120.00, 142.00, 145.00, 156.00	Superseded by Patch 175.00
Patches 33.00, 49.00, 50.00, 51.00, 52.00, 88.00, 100.00, 115.00, 121.00, 54.00, 161.00	Superseded by Patch 176.00

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

Patch 18.00	Superseded by Patch 179.00
Patch 5.00	Superseded by Patch 184.00
Patch 6.00	Superseded by Patch 185.00
Patches 64.00, 74.00, 199.00	Superseded by Patch 200.00
Patch 58.00, 73.00, 180.00	Superseded by Patch 210.00

**Table 2–2: Summary of Base Operating System Patches**

Patch IDs	Abstract
Patch 2.00 OSF440CDE-002	<p><b>Patch:</b> Security (SSRT0571U)  <b>State:</b> Supersedes patch OSF440CDE-001 (1.00)  This patch corrects the following:</p> <ul style="list-style-type: none"> <li>• A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability.</li> <li>• 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.</li> </ul>
Patch 3.00 OSF440CDE-003	<p><b>Patch:</b> Security (SSRT0585U)  <b>State:</b> 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.</p>
Patch 4.00 OSF440CDE-004	<p><b>Patch:</b> Security (SSRT0580U)  <b>State:</b> 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.</p>
Patch 7.00 OSF440DX-001	<p><b>Patch:</b> dxcalendar Reminder Displays Through dxpause Screen  <b>State:</b> Existing  This patch fixes the problem where the dxcalendar reminder displays through the pause screen (dypause) and remains on the top of the pause window.</p>
Patch 8.00 OSF440-010	<p><b>Patch:</b> Fix For POP Mail Handler  <b>State:</b> Existing  This patch corrects the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• The POP mail handler fails to properly rename its temp file after receiving a quit command.</li> </ul>
Patch 11.00 OSF440-013	<p><b>Patch:</b> Security (SSRT0596U)  <b>State:</b> 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.</p>

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

---

Patch 17.00 OSF440-019	<b>Patch:</b> Fix For BIND Server <b>State:</b> Existing This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes a problem in which a BIND server writes files to the /etc/namedb directory instead of the /var/tmp directory.</li></ul>
Patch 19.00 OSF440-020	<b>Patch:</b> Fix For yacc <b>State:</b> 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	<b>Patch:</b> Cannot Use ipcs Cmd On System Not Booted With vmunix <b>State:</b> 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	<b>Patch:</b> Fix For XTI And DECnet/OSI <b>State:</b> Supersedes patch OSF440-016A (14.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>
Patch 22.00 OSF440-024	<b>Patch:</b> automount Daemon Hangs <b>State:</b> Existing This patch fixes a problem in which the automount daemon hangs when invoked by the rsh command.
Patch 26.00 OSF440-029	<b>Patch:</b> Fix For defragment -V Option <b>State:</b> Existing This patch fixes a problem with the defragment command, where the -V option is not being parsed properly.
Patch 28.00 OSF440-030	<b>Patch:</b> Security (SSRT0556U) <b>State:</b> 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	<b>Patch:</b> mkdir -p Not Returning Error <b>State:</b> 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	<b>Patch:</b> Fix For kio Subsystem Panic <b>State:</b> 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 35.00 OSF440-040	<b>Patch:</b> Enhancement For verify Utility <b>State:</b> Existing This enhancement for the /sbin/advfs/verify utility allows it to detect loops in the list of free frags kept in the frags file.
Patch 36.00 OSF440-041	<b>Patch:</b> volrootmir -a Cmd Fails <b>State:</b> Existing This patch fixes a problem wherer the LSM command volrootmir -a fails if the source and target disks are not the same type.
Patch 37.00 OSF440-042	<b>Patch:</b> volrecover Not Returning Failed Status Code <b>State:</b> 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	<b>Patch:</b> quotaon Returns Incorrect Error Status <b>State:</b> 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	<b>Patch:</b> binmail Delivers Only Partial Messages <b>State:</b> Existing This patch fixes binmail to prevent partial delivery of mail messages when disk quota is reached.
Patch 41.00 OSF440-047A	<b>Patch:</b> Fix For nroff Y2K Problem <b>State:</b> 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 42.00 OSF440-048	<b>Patch:</b> Fixes For vrestore Command <b>State:</b> Existing This patch fixes two problems with the vrestore command. First, the command was slow to complete when a partial restore operation was requested. Second, the command failed to ignore extended attribute records for the files that were not requested for a vrestore operation.
Patch 43.00 OSF440-049	<b>Patch:</b> Fix For XTI Over TCP/IP <b>State:</b> 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 44.00 OSF440-005	<b>Patch:</b> Fix For Kernel Memory Fault <b>State:</b> Existing This patch fixes a kmf problem in bucket 2 (64-byte bucket ) when the type of SCSI device dynamically changes.
Patch 45.00 OSF440-051	<b>Patch:</b> Fix For sort -i Abort Problem <b>State:</b> Existing This patch fixes a problem in which sort -i a_file >b_file aborts with the message "A line of the input file contains more than 20480 characters." when LANG = da_DK.ISO8859-1.
Patch 46.00 OSF440-052A	<b>Patch:</b> Shared Library Fix For curses-based Applications <b>State:</b> 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.

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

Patch 47.00 OSF440-053	<b>Patch:</b> vi Puts Server Port INTO PASSALL MODE <b>State:</b> Existing This patch 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.
Patch 53.00 OSF440-006	<b>Patch:</b> Fix For spo_process_rsp Panic <b>State:</b> Existing This patch 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!")
Patch 59.00 OSF440-007	<b>Patch:</b> Characters Randomly Repeated Using tip <b>State:</b> Existing This patch corrects the following: <ul style="list-style-type: none"><li>• When using tip or any other method over the serial com lines to a receiver that sends frequent xoff/xon, characters are randomly repeated.</li><li>• 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.</li></ul>
Patch 60.00 OSF440-008	<b>Patch:</b> Fix For spo_misc_errors errlog Entries <b>State:</b> Existing This patch fixes the cause of the spurious spo_misc_errors errlog entry on 4100 class systems.
Patch 61.00 OSF440X11-001	<b>Patch:</b> Enhancement For makedepend Utility <b>State:</b> Existing This patch increases the maximum number of files that one file can depend on in the makedepend utility from 1024 to 4096.
Patch 62.00 OSF440X11-002A	<b>Patch:</b> Fix For Motif Drag-and-Drop <b>State:</b> Existing This patch 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.
Patch 63.00 OSF440X11-003	<b>Patch:</b> xfs Fails With Segmentation Fault <b>State:</b> Existing This patch fixes a problem where the X font server (xfs) often failed with a segmentation fault when it received an invalid request.
Patch 66.00 OSF440-023B	<b>Patch:</b> libxti/libtli Static Library Fix <b>State:</b> Supersedes patch OSF440-016B (65.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>
Patch 67.00 OSF440-033B	<b>Patch:</b> mount Cmd Sometimes Kills Other Processes <b>State:</b> Existing This patch fixes a problem with the mount command where it sometimes kills other processes.

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

Patch 68.00 OSF440-047B	<b>Patch:</b> nroff Incorrectly Translates Years After 1999 <b>State:</b> 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	<b>Patch:</b> Static Library Fix For curses-based Applications <b>State:</b> 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 70.00 OSF440X11-002B	<b>Patch:</b> libXm Static Library Fix For Motif Drag-and-Drop <b>State:</b> Existing This patch 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.
Patch 71.00 OSF440-054B	<b>Patch:</b> Ladebug Enhancements <b>State:</b> Existing This patch fixes problems in the DECthreads library for Tru 64 UNIX. Included in this patch are changes to support Ladebug enhancements and a bug fix for applications that employ SCS threads of different priorities.
Patch 72.00 OSF440-078	<b>Patch:</b> Updates FORE ATM (lfa) driver to Rev. V1.0.14 <b>State:</b> Existing This patch updates the FORE ATM (lfa) driver to Revision V1.0.14.
Patch 75.00 OSF440-060B	<b>Patch:</b> chvol Read & Write Transfer Size Increased <b>State:</b> Existing This patch corrects the following: <ul style="list-style-type: none"><li>• AdvFS volumes were not setting the default I/O byte transfer size to the preferred size reported by the disk drives.</li><li>• AdvFS chvol read and write transfer size range was increased.</li><li>• The read-ahead algorithm was modified to improve performance under certain conditions.</li></ul>
Patch 76.00 OSF440-001	<b>Patch:</b> Fix for simple lock panic <b>State:</b> New This patch fixes a system panic with the following panic string:  simple_lock: time limit exceeded
Patch 77.00 OSF440-100	<b>Patch:</b> tapex -L command reports failures <b>State:</b> New This patch 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.
Patch 78.00 OSF440-101	<b>Patch:</b> Fix for dbx <b>State:</b> New This patch fixes a problem in viewing a variable subrange parameter from a Pascal module while using dbx.

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

Patch 80.00 OSF440-103	<b>Patch:</b> Fix for cdfs file system <b>State:</b> New 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 end of partition. Only new and non-DEC CD-ROM drives are affected.
Patch 82.00 OSF440-106	<b>Patch:</b> Fix for system crash <b>State:</b> New 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 84.00 OSF440-108	<b>Patch:</b> Fix for ALPHAVME320 systems <b>State:</b> New This patch fixes two separate problems on the ALPHAVME320 platform: <ul style="list-style-type: none"><li>• Data corruption in the VB backplane driver.</li><li>• No floppy support in the platform code. The following error message is received during the boot when the floppy is configured at irq6:  EBV16, invalid isa0 irq6</li></ul>
Patch 85.00 OSF440-109	<b>Patch:</b> Security (SSRT0567U, SSRT0590U) <b>State:</b> Supersedes patch OSF440-014 (12.00) 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 86.00 OSF440-110	<b>Patch:</b> Fix for kernel memory fault <b>State:</b> New This patch fixes a kernel memory fault caused by a mishandling of multicast addresses on the FDDI interface.
Patch 87.00 OSF440-111	<b>Patch:</b> DECthreads Library Fix <b>State:</b> Supersedes patch OSF440-054A (48.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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 that employ SCS threads of different priorities.</li><li>• 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.</li></ul>
Patch 89.00 OSF440-113	<b>Patch:</b> Fix for ASE or Cluster system crash <b>State:</b> New This patch fixes system crashes seen on ASE or Cluster systems when changing the network interfaces. The stack is not informative and the panic may be "trap: illegal instruction" or "kernel memory fault."

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

---

Patch 93.00 OSF440-117	<b>Patch:</b> Fix for kdbx <b>State:</b> New. Supersedes patch OSF440-104B (201.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash.</li><li>• 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.</li></ul>
Patch 94.00 OSF440-118	<b>Patch:</b> MC1 or 1.5 will not configure <b>State:</b> New This patch 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.
Patch 98.00 OSF440-122A	<b>Patch:</b> Fix for C++ compiler tools <b>State:</b> New This patch 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.
Patch 101.00 OSF440-126	<b>Patch:</b> Fix for prof -pixie -asm command <b>State:</b> New. Supersedes patch OSF440-122B (202.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes a problem where prof -pixie -asm would dump core if the executable being profiled contains extremely long symbol names.</li></ul>
Patch 104.00 OSF440-130	<b>Patch:</b> System hang prevents rlogins or telnets <b>State:</b> New This patch fixes a problem where systems could hang in the audit code, preventing rlogins or telnets into it.
Patch 105.00 OSF440-131A	<b>Patch:</b> Fix for class_admin class_daemon problem <b>State:</b> New 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 108.00 OSF440-134	<b>Patch:</b> Fixes several DEC C compiler problems <b>State:</b> New This patch corrects the following: <ul style="list-style-type: none"><li>• A compiler problem that allowed the generation of EV67 (CIX) instructions to be generated when using the -arch ev6 switch.</li><li>• A compile time performance problem with a very large (1.6 MB) array initialization.</li><li>• An optimization problem that caused incorrect output when using a signed char in a strcpy-like routine, if compiled using -O4 or higher.</li><li>• A compile time error for a source line such as a = strcpy(b,c) + 7.</li><li>• An optimizer problem that caused an unintended sign-extension in the Perl program. This caused an "op/pack" failure in test 9.</li></ul>

---

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

---

Patch 111.00 OSF440-137	<b>Patch:</b> System panics with kernel memory fault msg in dqget <b>State:</b> New This patch fixes a problem where the system can panic with a "kernel memory fault" in dqget.
Patch 114.00 OSF440-140	<b>Patch:</b> Fix for NFS system hang <b>State:</b> New. Supersedes patch OSF440-135 (109.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes a system hang problem due to a bug in the NFS write gathering code. The code does not fully synch all writes.</li><li>• Fixes a problem where applications on V4.0F systems can hang, looping in readdirplus().</li></ul>
Patch 118.00 OSF440-144	<b>Patch:</b> Security (SSRT0563U) <b>State:</b> 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) This patch corrects the following: <ul style="list-style-type: none"><li>• There was a problem where process accounting data was not written to the accounting file when it was on an NFS-mounted file system.</li><li>• Corrects a "simple_lock: time limit exceeded" panic in softclock_scan().</li><li>• 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.</li><li>• Corrects a problem where a signal is delivered, but not responded to, by the target process.</li><li>• Fixes a panic of "get_color_bucket: empty buckets" when the sysconfig attribute "private-cache-percent" is non-zero.</li><li>• A potential security vulnerability has been discovered where under certain circumstances users may gain unauthorized access. Compaq has corrected this potential vulnerability.</li><li>• Fixes a problem with the mount command where it sometimes kills other processes.</li><li>• 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.</li><li>• Fixes problems with loadable drivers indicated by a maximum device number, lack of device number 0, or failure to reconfigure or reload a driver.</li><li>• Fixes a problem in which mount would incorrectly fall back to Version 2 after certain errors had been encountered using Version 3.</li><li>• Fixes an nfs/ufs/vm deadlock. While serving a client, the system running ASE/DT as an NFS server can hang with deadlock.</li><li>• Fixes a problem in which the system may panic with the error message "kernel memory fault".</li></ul>

---

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

---

Patch 118.00 continued	<ul style="list-style-type: none"><li>• Fixes several KZPCC RAID controller problems which in turn provides full support of the product.</li><li>• Fixes a problem where applications using the fcntl() system calls may appear to hang.</li><li>• Fixes "simple_lock: time limit exceeded" panics.</li><li>• Fixes two problems; fork can fail to obtain swap space and the resource limitation on core files does not work as documented.</li><li>• Fixes a problem where the system can panic with the following console message:  bs_bf_htop: invalid handle\n N1 = 0</li><li>• Fixes a system "pause" seen when doing a lot of I/O to UFS filesystems.</li><li>• 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.</li><li>• This work provides functionality to allow detecting unlinked referenced files. This work is in response to a Citibank ECP.</li><li>• Fixes a problem with the map entry indexing scheme that results in the following panic:  pmap_release_page: page not found</li><li>• 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.</li><li>• 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.</li><li>• Fixes a problem in the module core() that can cause a panic with the message:  vrel: bad ref count</li><li>• Fixes two separate problems:<ul style="list-style-type: none"><li>– A panic in the kernel with the following error message:  simple_lock: time limit exceeded</li><li>– A panic occurs when booting kernel interactively and setting the memlimit. The panic error message is as follows:  kernel memory fault</li></ul></li><li>• Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash.</li><li>• 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.</li><li>• Fixes several problems associated with Controller Reset (hard-error recovery) for the KZPCC backplane RAID controller.</li><li>• Fixes a system hang condition. All NFS-related services may deadlock.</li></ul>
---------------------------	--

---

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

Patch 119.00 OSF440-145	<b>Patch:</b> System hang occurs in I2c code <b>State:</b> New This patch fixes a intermittent hang occurring in the I2c code. This hang is most commonly seen on the DS10 workstation.
Patch 123.00 OSF440-149A	<b>Patch:</b> libsecurity shared library produces core file <b>State:</b> New This patch fixes a problem of libsecurity producing a core file when handling error conditions.
Patch 124.00 OSF440-150A	<b>Patch:</b> libots3 shared run-time library fix <b>State:</b> New 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	<b>Patch:</b> Security (SSRT0583Z) <b>State:</b> 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 128.00 OSF440-154	<b>Patch:</b> Fix and update for sys_check utility <b>State:</b> New This patch provides bug fixes to the sys_check utility and updates the sys_check to version 114.
Patch 131.00 OSF440-159	<b>Patch:</b> Fixes for Compaq AlphaServer DS20E and DS20 <b>State:</b> New. Supersedes patch OSF440-107 (83.00) This patch corrects the following: <ul style="list-style-type: none"><li>• When configuring the AlphaServer ES40, the ISA devices IDE and USB are not configured if a combo card is installed.<ul style="list-style-type: none"><li>– On the ES40 and DS20, nonfatal 680 environment machine checks are being logged as fatal/noncorrectable errors.</li><li>– On the DS20, a fix has been made to the handling of power supply, temperature, and fan events so that they are reported correctly.</li><li>– Provides support for the Compaq AlphaServer DS20E.</li></ul></li><li>• System panics with a kernel memory fault when installing on a AlphaServer DS20.</li><li>• Fixes the following Compaq AlphaServer problems:<ul style="list-style-type: none"><li>– On the ES40 and DS20, nonfatal 680 environment machine checks are being logged as fatal/noncorrectable errors.</li><li>– On the DS20, a fix has been made to the handling of power supply, temperature, and fan events so that they are reported correctly.</li><li>– Provides support for the Compaq AlphaServer DS20E.</li></ul></li></ul>
Patch 132.00 OSF440-160	<b>Patch:</b> Fix for packetfilter applications <b>State:</b> New This patch fixes a problem with packetfilter applications that use IP packets greater than 8 K.
Patch 135.00 OSF440-021	<b>Patch:</b> Fix for ar command <b>State:</b> New This patch eliminates the previous limitation on the maximum number of external symbols that could be handled by the ar command.

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

---

Patch 136.00 OSF440-025	<b>Patch:</b> Fix for assert panic <b>State:</b> New This patch corrects the following: <ul style="list-style-type: none"><li>• Callback thread blocking forever in <code>isp_enable_lun</code></li><li>• <code>assert wait</code> in <code>xpt_ccb_alloc panic</code></li></ul>
Patch 139.00 OSF440-037	<b>Patch:</b> Fix for lock-terminate system panic <b>State:</b> New 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.
Patch 140.00 OSF440-038	<b>Patch:</b> Fixes a problem with the <code>newfs</code> command <b>State:</b> New. Supersedes patch OSF440-121 (97.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes invalid <code>malloc</code> message in <code>mfs</code>.</li><li>• - Fixes a problem with the <code>newfs</code> command. When the <code>newfs -N</code> command was run on a mounted file system, it returned an error message similar to the following:  <code>newfs: /dev/rz0c: is marked in the disklabel as in use by: 4.2BSD</code></li></ul>
Patch 144.00 OSF440-064	<b>Patch:</b> Fix for NFS problems <b>State:</b> New This patch corrects the following: <ul style="list-style-type: none"><li>• When starting or stopping NFS, NFS was not checking for NFS daemons running.</li><li>• <code>rpc.pcnfsd</code> was causing core dumps when receiving a <code>SIGTERM</code> signal.</li></ul>
Patch 147.00 OSF440-068	<b>Patch:</b> Fixes a problem with creating multiple ATM ELANs <b>State:</b> New This patch fixes a problem with the creation of multiple ATM ELANS.
Patch 148.00 OSF440-069	<b>Patch:</b> Fix for <code>rsh</code> hang <b>State:</b> New This patch fixes <code>rsh(1)</code> hanging forever in <code>select()</code> .

---

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

---

Patch 151.00 OSF440-072	<p><b>Patch:</b> Fix for ITPSA driver</p> <p><b>State:</b> Supersedes patches OSF440-062 (56.00), OSF440-119 (95.00), OSF440-129 (103.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• Fixes a problem in which a system with a KZPCA host bus adapter may hang when the SCSI bus is reset.</li><li>• 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 event log.</li><li>• Fixes the following problems related to the ITPSA driver that supports the KZPCM adapter:<ul style="list-style-type: none"><li>– 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.</li><li>– Errors can occur while the system is processing a SCSI bus or SCSI bus device reset request that is issued from the class driver.</li><li>– On the 8951U and 8952U adapters, SCSI bus resets are lost when these adapters are connected to single-ended drives.</li><li>– A panic can occur during boot when lockmode is set to 4.</li></ul></li><li>• Fixes a problem with the ITPSA driver for KZPCM and KZPCA devices, which resulted in a synchronization problem, causing the SCSI bus to hang.</li></ul>
Patch 152.00 OSF440-073	<p><b>Patch:</b> System hang with large number of pending ioctls</p> <p><b>State:</b> Supersedes patches OSF440-018 (16.00), OSF440-157 (130.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• Fixes a kernel memory fault caused by a streams SMP race condition.</li><li>• Fixes the following Universal Serial Bus (USB) problems:<ul style="list-style-type: none"><li>– The USB mouse no longer functions after resetting the Xserver.</li><li>– System panics may occur in error handling after a USB device fails a request.</li><li>– The USB device may not deconfigure properly when unplugged from the bus.</li><li>– Problems that will prevent some USB devices from being configured at boot time.</li><li>– A key on a USB keyboard will continue to repeat after being unplugged.</li><li>– USB keyboards may transmit the incorrect keycode for several keys.</li></ul></li><li>• Fixes a system hang in which there is a large number of pending ioctls on the streams queue.</li></ul>
Patch 153.00 OSF440-074	<p><b>Patch:</b> Fixes a problem within the SCSI and tape subsystems</p> <p><b>State:</b> New</p> <p>This patch fixes a problem within the SCSI and tape subsystems, in which an expression was not being evaluated properly.</p>

---

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

---

Patch 154.00 OSF440-075	<b>Patch:</b> Fixes restart detection problem with proplistd <b>State:</b> Supersedes patch OSF440-063 (57.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Corrects several NFS problems. Specifically, it fixes a problem where NFS does not update mtime and atime for special files and named pipes. Additionally, it fixes a problem that can cause an NFS client application to hang, or causes a "lock already owned by thread" panic when lockmode=4. The patch also fixes a problem where incorrect NFS client locking caused a KFM panic. Finally the patch fixes a problem where NFS clients may hang in the uninterruptable state.</li><li>• 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.</li></ul>
Patch 158.00 OSF440-079	<b>Patch:</b> Error message added to DHCP for outdated databases <b>State:</b> New This patch 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.
Patch 159.00 OSF440-080	<b>Patch:</b> : Fix for system hang with inetd <b>State:</b> New 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.
Patch 162.00 OSF440-083	<b>Patch:</b> Fix for unresolved symbol:scc_configure message <b>State:</b> New This patch fixes a problem in which systems that use the 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 165.00 OSF440-087	<b>Patch:</b> Fixes a problem with CDFS <b>State:</b> Supersedes patch OSF440-044 (39.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes a problem where a system panic will occur when accessing an ISO-9660 format CDROM.</li><li>• Fixes a problem with CDFS. Data corruption occurs when reading beyond the end of a partition.</li></ul>
Patch 167.00 OSF440-089	<b>Patch:</b> Fix for vdump core dump problem <b>State:</b> New This patch fixes a problem where the vdump program would dump core with the following message:  nnnn Resources lost(coredump)
Patch 168.00 OSF440-009	<b>Patch:</b> Corrects the printing of Japanese SJIS strings <b>State:</b> New. Supersedes patch OSF440-114 (90.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Corrects how the C shell handles 2-byte characters when running in the Japanese SJIS locale.</li><li>• Corrects the printing of Japanese SJIS strings that are assigned to shell variables in the C shell (csh).</li></ul>

---

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

---

Patch 169.00 OSF440-090	<b>Patch:</b> Fix for crontab -e user command <b>State:</b> New 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	<b>Patch:</b> Fixes a problem with the stdhosts command <b>State:</b> New 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 173.00 OSF440-094	<b>Patch:</b> fsck may not be able to repair UFS filesystem <b>State:</b> New. Supersedes patch OSF440-115 (91.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes and enhances the quotacheck and fsck commands.</li><li>• Fixes a problem in which the fsck utility may be unable to repair a UFS filesystem.</li></ul>

---

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

---

Patch 175.00 OSF440-096	<p><b>Patch:</b> Fix for data loss problem that occurs with ksh</p> <p><b>State:</b> 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)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• Fixes a problem with /usr/bin/ksh and the named-pipe (FIFO) communication that is used by applications.</li><li>• 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.</li><li>• ksh does a segmentation fault and core dumps when displaying a here-document.</li><li>• Fixes problems in ksh, file, tail, nawk, awk, and pax.<ul style="list-style-type: none"><li>– Unexpected logouts and terminal hangups occur when using the /bin/su command and /bin/ksh as a login shell.</li><li>– The file command gives incorrect output concerning WAV audio files.</li><li>– The tail command gives erroneous output when used with both the -n and -r flags.</li><li>– The maximum number of fields per record was changed from 99 to 199 for the awk command.</li><li>– 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.</li></ul></li><li>• Fixes a problem in ksh which required two SIGTERM signals to be sent to the process when it exec'ed.</li><li>• Corrects a problem that may cause ksh to coredump when displaying a large here-document in a ksh script.</li><li>• - Fixes a problem that caused incorrect file dates to be restored when pax was used to copy files.<p>The problem occurred in the following cases:</p><ul style="list-style-type: none"><li>– If the file was a nonempty directory</li><li>– If the file was the target of another symbolic link</li></ul></li><li>• Fixes a core dump from ksh.</li><li>• Fixes a problem with the Korn shell where data loss occurs when commands are piped together.</li></ul>
----------------------------	---

---

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

---

Patch 176.00 OSF440-097A	<p><b>Patch:</b> Fix for log_flush_sync system panic</p> <p><b>State:</b> Supersedes patches 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)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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</li><li>• Fixes an AdvFS domain panic that occurs with the following message on the console:  load_x_cache: bad status from bs_refpg of sbm</li><li>• Fixes a problem with AdvFS that will cause the system to panic with "kernel memory fault" in audit_rec_build().</li><li>• 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).</li><li>• Provides the following fixes and enhancements to AdvFS:<ul style="list-style-type: none"><li>– AdvFS volumes were not setting the default I/O byte transfer size to the preferred size reported by the disk drives.</li><li>– AdvFS chvol read and write transfer size range was increased.</li><li>– The read-ahead algorithm was modified to improve performance under certain conditions.</li></ul></li><li>• 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</li><li>• Fixes a problem where update takes too long to sync mmap files when using an AdvFS file system.</li><li>• Fixes the following two problems in AdvFS:<ul style="list-style-type: none"><li>– When a log half full or log full" problem occurs, an entire system will panic.</li><li>– 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.</li></ul></li><li>• 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.</li><li>• 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.</li><li>• 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</li></ul>
-----------------------------	--

---

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

---

Patch 177.00 OSF440-098	<b>Patch:</b> portmap allows RPC select timeouts to occur <b>State:</b> New. Supersedes patches OSF440-102 (79.00), OSF440-151 (125.00), OSF440-035 (138.00), OSF440-093 (172.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Modifies the strftime() function to make the %V format specifier return the correct week.</li><li>• Fixes a problem of password error messages not being displayed during installation of the security subsystem.</li><li>• 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.</li><li>• Fixes problems with rsh(1), rlogin(1), and rcp(1) if netgroup names are defined with uppercase letters.</li><li>• Fixes a problem with portmap by allowing RPC select() timeouts to occur when interrupted by signals.</li></ul>
Patch 179.00 OSF440-192	<b>Patch:</b> Fix for panics on AlphaServer GS140/GS60 systems <b>State:</b> Supersedes patch OSF440-002 (18.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Resolves corrupt EV6 binary error log entries for IOP detected UDE (Uncorrectable Data Error) packets on AlphaServer 8200/8400 platforms.</li><li>• Fixes a problem on some AlphaServer GS140/GS60 configurations where a simple lock timeout or TB shoot ack timeout panic may occur.</li></ul>
Patch 181.00 OSF440-216	<b>Patch:</b> Fix for system panic with tcp_output REXMT error msg <b>State:</b> New. Supersedes patches OSF440-116 (92.00), OSF440-070 (149.00), OSF440-071 (150.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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 of the following form when the error is encountered: <pre>&gt;&gt;May 25 12:29:17 dragon pppd[2525]: ioctl(SIOCDIFADDR): Invalid argument</pre></li><li>• Fixes a kernel memory fault and an SMP race condition with the AltaVista Firewall 98 server on a multi-CPU system.</li><li>• Fixes a problem when a default IP address and a cluster virtual IP address get interchanged after a network restart. The default interface address is used by all outgoing traffic and the alias address can only be used for the incoming packets.</li><li>• Fixes a problem in which the system may panic with the error message "tcp_output REXMT".</li></ul>
Patch 182.00 OSF440CDE-010	<b>Patch:</b> Fix for X server color map problem <b>State:</b> New 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	<b>Patch:</b> Security (SSRT0614U) <b>State:</b> 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 184.00 OSF440CDE-007	<b>Patch:</b> dtfile does not work correctly in restricted mode <b>State:</b> Supersedes patch OSF440CDE-005 (5.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes a problem where the CDE File Manager (dtfile) sometimes left defunct processes.</li><li>• Fixes a problem where the Common Desktop Environment (CDE) File Manager (dtfile) did not work correctly in restricted mode.</li></ul>
Patch 185.00 OSF440CDE-008	<b>Patch:</b> Security (SSRT0600U) <b>State:</b> Supersedes patch OSF440CDE-006 (6.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>
Patch 186.00 OSF440CDE-009A	<b>Patch:</b> Fix for dxaccounts error message <b>State:</b> New 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	<b>Patch:</b> diskconfig fails when creating an AdvFS partition <b>State:</b> New. Supersedes patch OSF440DX-007 (192.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes a problem with the diskconfig utility where ri type disks were not correctly recognized.</li><li>• 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</li></ul>
Patch 188.00 OSF440DX-003	<b>Patch:</b> Compaq SCSI SNMP sub-agent returns incorrect info <b>State:</b> New 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.

---

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

---

Patch 193.00 OSF440DX-008	<b>Patch:</b> usermod does not allow commas in comma field <b>State:</b> New. Supersedes patches OSF440DX-004 (189.00), OSF440DX-005 (190.00), OSF440DX-006 (191.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes two situations in which the GUI account management program (dxaccounts) will crash in a Enhanced Security client environment when attempting to copy a NIS user account.</li><li>• 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 newline character (\n).</li><li>• Fixes a problem where usermod -D can coredump if an NIS group entry contains a large number of users.</li><li>• Fixes a problem in which the usermod command was not allowing any commas in the comment field when the current GECOS fields are filled.</li></ul>
Patch 194.00 OSF440DX-009	<b>Patch:</b> Security (SSRT0612U) <b>State:</b> 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 195.00 OSF440X11-005A	<b>Patch:</b> Shared library fix for libXt <b>State:</b> New This patch fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt).
Patch 196.00 OSF440X11-006	<b>Patch:</b> XDMCP Indirect queries do not work <b>State:</b> New This patch fixes a problem in the X Display Manager (xdm) where XDMCP Indirect queries do not work.
Patch 198.00 OSF440X11-008	<b>Patch:</b> X server crashes when viewing TIFF images <b>State:</b> New This patch fixes a problem where viewing certain TIFF images with an image viewer crashed the X server.
Patch 200.00 OSF440X11-015	<b>Patch:</b> X server support for PCI To Ethernet/Graphics adapter <b>State:</b> Supersedes patches OSF440X11-004 (64.00), OSF440X11-007 (74.00), OSF440X11-009 (199.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes a problem where on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the X server does not draw lines correctly.</li><li>• 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).</li></ul>
Patch 203.00 OSF440-149B	<b>Patch:</b> libsecurity static library produces core file <b>State:</b> New This patch fixes a problem of libsecurity producing a core file when handling error conditions.

---

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

---

Patch 204.00 OSF440-150B	<b>Patch:</b> libots3 static run-time library fix <b>State:</b> New 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	<b>Patch:</b> Fix for dxaccounts BadPixmap error <b>State:</b> New 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 206.00 OSF440X11-005B	<b>Patch:</b> Static library fix (libXt) <b>State:</b> New This patch fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt).
Patch 208.00 OSF440-231	<b>Patch:</b> Support for New Hardware Delivery Two (NHD2) <b>State:</b> New. Supersedes patches OSF440-139 (113.00), OSF440-230 (207.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes a problem where the linker (ld) would insert incorrect values for the symbols etext and _etext when building kernels larger than 4 MB.</li><li>• 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.</li></ul>

---

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

---

Patch 209.00 OSF440-131B	<b>Patch:</b> Static library fix for libclass.a <b>State:</b> New 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 210.00 OSF440-239	<b>Patch:</b> Updates emx Fiber Channel driver to revision 1.12 <b>State:</b> Supersedes patches OSF440-088 (73.00), OSF440-065 (58.00), OSF440-207 (180.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes various problems with the driver support for the Powerstorm 4D10T (ELSA Gloria Synergy) graphics board.</li><li>• - 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).</li><li>• This patch updates the emx Fiber Channel driver to revision 1.12, adds support for the KGPSA-CA adapter, and it also fixes the following problems:<ul style="list-style-type: none"><li>– 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.</li><li>– When connected to the new Pleiades II switches, the switch ports would consume target ids on the adapter's scsci bus.</li><li>– A kernel memory fault in routine emx_handle_els_request.</li><li>– A system hang at boot up caused by infinitely trying to probe the Fiber Channel link.</li></ul></li><li>• Adds additional error detection to the FC driver.</li></ul>

---

---

## Summary of TruCluster Software Patches

This chapter summarizes the TruCluster software patches included in Patch Kit-0002.

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 5.00, 6.00, 8.00	New
Patch 1.00	Superseded by Patch 7.00

**Table 3–2: Summary of TruCluster Patches**

Patch IDs	Abstract
Patch 2.00 TCR160-002	<p><b>Patch:</b> Fix For asedirector  <b>State:</b> Existing            This patch corrects the following:</p> <ul style="list-style-type: none"> <li>Fixes an ASE command timeout problem encountered by large ASE services.</li> <li>Fixes an incorrect decision made by the asedirector as a result of a failed inquire services command.</li> </ul>
Patch 3.00 TCR160-003	<p><b>Patch:</b> DRD Permissions May Be Lost  <b>State:</b> Existing            This patch fixes a problem where DRD permissions could be lost if a service is modified more than once.</p>
Patch 4.00 TCR160-004	<p><b>Patch:</b> Fix for Kernel Memory Fault On DRD Client Nodes  <b>State:</b> 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.</p>
Patch 5.00 TCR160-007	<p><b>Patch:</b> ASE agent loops during start or stop of service  <b>State:</b> New            This patch fixes an ASE problem where under certain circumstances the service scripts could cause the ASE agent to loop during a start or stop service.</p>
Patch 6.00 TCR160-008	<p><b>Patch:</b> Fix for cluster node panic  <b>State:</b> New            This patch fixes a problem in which a cluster node can panic with the panic string "convert_lock: bad lock state".</p>

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

---

Patch 7.00 TCR160-010	<b>Patch:</b> Fix for Reliable Datagram API <b>State:</b> Supersedes patch TCR160-001 (1.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Reliable Datagram (RDG) messaging support.</li><li>• RDG: bug fix to the completion queue synchronization protocol.</li></ul>
Patch 8.00 TCR160-011	<b>Patch:</b> doconfig may hang when running in TruCluster environment <b>State:</b> New This patch fixes two problems that could cause doconfig to appear to hang when running in a TruCluster environment.

---