# DIGITAL UNIX 3.2G, Available Server Environment 1.3, and TruCluster 1.0

## Patch Summary and Release Notes for Patch Kit-0005

**March 1999**

This manual describes the release notes and contents of Patch Kit-0005. It provides any special instructions for installing individual patches.

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

**Compaq Computer Corporation**
**Houston, Texas**

# Contents

# About This Manual

This manual contains information specific to Patch Kit-0005 for the DIGITAL UNIX Version 3.2G operating system, TruCluster Version 1.0 software products, and Available Server Environment Version 1.3. 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 Available Server Environment patches included in the kit.

Chapter 3 Summarizes the base operating system patches included in the kit.

Chapter 4 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 DIGITAL UNIX, TruCluster, and Available Server Environment documents:

- DIGITAL UNIX, ASE, and TCR *Patch Kit Installation Instructions*
- DIGITAL UNIX *Installation Guide*
- DIGITAL 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 DIGITAL 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 DIGITAL UNIX that you are using.
- If known, the type of processor that is running the DIGITAL UNIX software.

The DIGITAL 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 DIGITAL UNIX 3.2G, TCR 1.5, and ASE 1.0 Patch Kit-0005.

## 1.1 Required Storage Space

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

### Available Server Environment

- 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 ~34.4 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 ~35.0 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 ~502 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

  A total of ~120 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

### 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 ~30.0 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 ~30.4 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 ~469 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 ~35.0 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 ~36.0 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 ~503 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~120 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 multi-product support within dupatch is most visible when installing or removing patches. dupatch will display a list of the products which 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 DIGITAL UNIX operating system, ASE, and TCR patch kits. An example of patch cross-product dependency handling for a system with both DIGITAL UNIX 3.2G and TCR 1.0 installed follows:

- If a DIGITAL UNIX 3.2G Patch 1.00 is chosen for installation and it depends upon TruCluster 1.0 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 DIGITAL UNIX 3.2G 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. The special instructions are now displayed when patches are removed. The per-patch special instructions are viewable 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 non-root 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 Baselining

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.

#### 1.2.5.1 Known Problem with Patch Baseline Analysis/Adjustment

There is a known problem when running Patch Baseline Analysis/Adjustment, selection 5, from the dupatch main menu.

This will not block the installation of any patches.

The following is a section from the Patch Baseline Analysis/Adjustment output showing missing hardlink to and files. This output should be ignored.

```
Phase 4 - Report changed system files and missing files
=======================================================

    This phase provides information to help you make choices later in
    this process.  It reports both 'missing' and files whose origin
    cannot be determined.  Some of these files may affect patch
    installation.  You will want to consider this information when you
    later make decisions in phase 5.

    * list of changed files with unknown origin:
      ----------------------------------------

  ./sbin/pax     OSFBASE375            UNKNOWN
      MISSING HARDLINK TO ./sbin/cpio.new
  ./sbin/sh      OSFPAT00042200375     UNKNOWN
      BROKEN HARDLINK TO ./sbin/Rsh
  ./sbin/Rsh     OSFPAT00042200375     UNKNOWN
      BROKEN HARDLINK TO ./sbin/sh
  ./sbin/tar     OSFBASE375            UNKNOWN
      MISSING HARDLINK TO ./sbin/cpio.new

    * list of "missing" files:
      -------------------------

  ./isl/sas/.profile               OSFBASE350      MISSING
  ./isl/sifsync                    OSFBASE350      MISSING
  ./usr/lib/emacs/lisp/term/.el    OSFEMACS350     MISSING
```

### 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 DIGITAL UNIX, ASE, and TCR). This switch allows you to specify the product name which 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, rev 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 Special Instructions for Patch 371.00

The printer log, lpr.log now reports the creation of files preceded by a dot (.) in the spooling directories. Do not amend or delete these files as the printer subsystem manages their creation and cleanup.

For initial use, DIGITAL recommends that you set the logging level to `lpr.info`. If you have a problem that is escalated to technical support, the support organization will request `lpr.log` at the `lpr.debug` level. This is because the DEBUG messages provide a detailed trace that can only be interpreted by reference to the source code and `lpr.log` will simply grow more quickly if DEBUG messages are logged. The `lpr.info` level provides a shorter report of an event, including any network retry messages and unusual occurences (which are not always errors).

All changes to the status file of a queue, including reports of any files printed, are reported at the DEBUG level rather than the INFO level. This reduces the rate of growth of the file and allows you to monitor and react to important events more quickly. The WARNING level logs events that may need to be attended to, while the ERROR level logs hard (often fatal) errors.

To modify the logging level, edit your `/etc/syslog.conf` file and change the `lpr` line to the required level, such as `lpr.info` as follows:

```
lpr.info /var/adm/syslog.dated
```

Use the `ps` command to find the PID for the `syslog` daemon, and the following command to re-start `syslogd`:

```
# kill -HUP
```

A new set of log files will be created in /var/adm/syslog.

## 1.4 Special Instructions for Patch 401.00

When you install Patch 401.00 you must enable it before NFS is started because it must perform configuration operations before client requests arrive.

To manually enable Patch 401.00, first rebuild the kernel, then issue the following commands::

```
% dbx -k /vmunix
   (dbx) patch stall_write_patch_enabled=1
 (dbx) quit
% reboot
```

## 1.5 Special Instructions for Patch 386.00

Because Patch 386.00 will overwrite the system's existing cam_data.c file, you will need to perform additional steps when installing the patch. The steps you take depend upon your system configuration. This section decribes the steps you must take.

Patch 386.00 also provides new support for several tape drives. For information about that support, see Section 1.6.

### 1.5.1 Select Appropriate Steps

Choose the following option that describes your system, then perform the indicated steps described in Section 1.5.2. In every case, you must rebuild the kernel and reboot the system:

#### Option A

You have a cam_data.c file containing customized device information. Follow the steps listed in **Case 1**.

#### Option B

You have CLC, OSMS/OSDS, and/or MME layered products and/or other products that make modifications to the cam_data.c file. Follow the steps listed in **Case 2**.

#### Option C

Your system matches both Option A and Option B on your system. Follow the steps listed in both **Case 1** and **Case 2**.

#### Option D

You have neither Option A nor Option B on your system. Follow the steps listed in **Case 3**.

### 1.5.2 Perform Appropriate Steps

The steps decribed in the following situations must be take before you install Patch 386.00 and continue after it is installed.

#### Case 1:

1. Back up the original cam_data.c file:

```
# cp -p /usr/sys/data/cam_data.c /usr/sys/data/cam_data.c.org
```

2. Install Patch 386.00.
3. Manually merge the original cam_data.c and the patched cam_data.c using the editor of your choice. The following steps assume that the patched cam_data.c file has been placed in a /patches directory:

   a. In window 1, edit the /usr/sys/data/cam_data.c.org file and select the customized information:

   ```
   # view /usr/sys/data/cam_data.c.org
   ```

   b. In window 2, copy /patches/cam_data.c into /usr/sys/data/cam_data.c

   ```
   # cp /patches/cam_data.c /usr/sys/data/cam_data.c
   ```

   c. Edit the /usr/sys/data/cam_data.c file:

   ```
   # vi /usr/sys/data/cam_data.c
   ```

   d. At the location where the customized information needs to be located, paste the selected information from window 1, save the changes, and exit the file.

4. If your system has CLC, OSMS/OSDS, and/or MME layered products and/or other products installed, proceed to Case 2. Otherwise, proceed to Section 1.5.3.

**Case 2:**

When CLC, OSMS/OSDS, and/or MME layered products and/or other products are installed, you will need to determine which products have changed the cam_data.c file. To do this, search the setld script files, as follows:

```
# grep cam_data.c /usr/.smdb./*.scp
```

With the exception of the OSFBINCOM375 subset (Base Operating System), any subset that is displayed has modified the cam_data.c file. If this applies, then perform the following steps:

1. Backup the original cam_data.c file:

   ```
   # cp -p /usr/sys/data/cam_data.c /usr/sys/data/cam_data.c.org
   ```

2. Deinstall the layered products/other products using the setld -d. For example:

   # **setld -d** [product_name]

3. Install Patch 386.00.
4. Reinstall the products that you deinstalled. See the appropriate installation guides.
5. Manually merge the original cam_data.c and the patched cam_data.c using the editor of your choice. The following steps assume that the patched cam_data.c file has been placed in a /patches directory:

   a. In window 1, edit the /usr/sys/data/cam_data.c.org file and select the customized information:

   ```
   # view /usr/sys/data/cam_data.c.org
   ```

b. In window 2, copy /patches/cam_data.c into /usr/sys/data/cam_data.c

```
# cp /patches/cam_data.c /usr/sys/data/cam_data.c
```

c. Edit the /usr/sys/data/cam_data.c file:

```
# vi /usr/sys/data/cam_data.c
```

d. At the location where the customized information needs to be located, paste the selected information from window 1, save the changes, and exit the file.

**Case 3:**

1. Backup the original cam_data.c file:

```
# cp -p /usr/sys/data/cam_data.c /usr/sys/data/cam_data.c.org
```

2. Install Patch 386.00.
3. Proceed to Section 1.5.3.

### 1.5.3 Rebuild the Kernel

Complete the following steps to rebuild the kernel. For more information, see the DIGITAL UNIX *Installation Guide*.

1. Backup the original /vmunix:

```
# cp /vmunix /vmunix.prepatch
```

If there is not enough space in the root directory, move the/vmunix patch file to a location in the /usr directory.

2. Run doconfig to create a new kernel:

```
# doconfig -c <system_name>
```

3. Copy the new /vmunix to the root directory:

```
# cp /sys/<system_name>/vmunix  /vmunix
```

4. Reboot the system:

```
# shutdown -r now
```

### 1.5.4 Restore Original Files

To restore the original configuration, you should be able to use the following steps.

1. Restore the original files:

```
# cp -p /usr/sys/data/cam_data.c.org /usr/sys/data/cam_data.c
```

```
# cp -p (location of backed up vmunix) /vmunix
```

2. Reboot the system:

```
# shutdown -r now
```

## 1.6 Patch 386.00 Support for Tape Drives

Patch 386.00 adds device recognition for several tape drives, including the TZ89, TZS20, and TLZ10. This section describes the media and format information for

these tape drives. For convenience, it includes this information for other tape drives, which is provided in the `tz`(7) Reference Page.

Table 1–1 lists the tape compatibility for various TZn tape drives.

**Table 1–1: Media Type for TZn Tape Drives**

| Media Type | Drive Type |
|---|---|
| CompacTapeI | TZ30, TK50 |
| CompacTapeII | TZ30, TK50, TK70, TZ85, TZ86 |
| CompacTapeIII | TZ85, TZ86, TZ87, TZ88, TZ89 |
| CompacTapeIIIXT | TZ88, TZ89 |
| CompacTapeIV | TZ88, TZ89 |

Table 1–2 provides information about TZ85, TZ86, TZ87, TZ88, and TZ89 tape drives. Note that in the capacity column, a number followed by an asterisk (*) assumes a 2:1 compression ratio. The actual compression ratio may vary depending on the type of data being compressed.

**Table 1–2: Supported Formats for TZn Tape Drives**

| Format | Device Special | Density Code | Compression | Capacity | Cartridge | I/O Supported |
|---|---|---|---|---|---|---|
| TZ85 | rmt?a | 1ah | N/A | 2.6 GB | CompacTape III | Read-only |
| TZ85 | rmt?l | 1ah | N/A | 2.6 GB | CompacTape III | Read-only |
| TZ86 | rmt?a | 1ah | N/A | 10.0 GB | CompacTape III | Read-only |
| TZ86 | rmt?l | 1ah | N/A | 10.0 GB | CompacTape III | Read-only |
| TZ87 | rmt?a | 1ah | Off | 10.0 GB | CompacTape III | Read-only |
| TZ87 | rmt?l | 1ah | On | 20.0 GB* | CompacTape III | Read-only |
| TZ87 | rmt?m | 00h | Off | 10.0 GB | CompacTape III | Read/write |
| TZ87 | rmt?h | 00h | On | 20.0 GB* | CompacTape III | Read/write |
| TZ88 | rmt?a | 1ah | Off | 15.0 GB | CompacTapeIIIXT | Read-only |
| TZ88 | rmt?l | 1ah | Off | 30.0 GB* | CompacTapeIIIXT | Read-only |
| TZ88 | rmt?m | 00h | Off | 15.0 GB | CompacTapeIIIXT | Read/write |
| TZ88 | rmt?h | 00h | On | 30.0 GB* | CompacTapeIIIXT | Read/write |
| TZ88 | rmt?a | 1ah | Off | 20.0 GB | CompacTape IV | Read/write |
| TZ88 | rmt?l | 1ah | On | 40.0 GB* | CompacTape IV | Read/write |
| TZ89 | rmt?a | 1ah | Off | 15.0 GB | CompacTapeIIIXT | Read-only |
| TZ89 | rmt?l | 1ah | Off | 30.0 GB* | CompacTapeIIIXT | Read-only |
| TZ89 | rmt?m | 00h | Off | 15.0 GB | CompacTapeIIIXT | Read/write |
| TZ89 | rmt?h | 00h | On | 30.0 GB* | CompacTapeIIIXT | Read/write |
| TZ89 | rmt?m | 00h | Off | 35.0 GB | CompacTape IV | Read/write |
| TZ89 | rmt?h | 00h | On | 70.0 GB* | CompacTape IV | Read/write |

Table 1–3 lists the tape compatibility for the TLZ04, TLZ06, TLZ07, TLZ09, and TLZ10 tape drives.

**Table 1–3: Tape Compatibility for TLZn Tape Drives**

| Media Type | Drive Type |
|---|---|
| DDS-1 (60m) | TLZ04, TLZ06, TLZ07, TLZ09, TLZ10 |
| DDS-1 (90m) | TLZ06, TLZ07, TLZ09, TLZ10 |
| DDS-2 (120m) | TLZ07, TLZ09, TLZ10 |
| DDS-3 (125m) | TLZ10 |

Table 1–4 provides information about the TLZ–family of tape drives. The TLZn tape drives support variable block size. Note that in the capacity column, a number followed by an asterisk (*) assumes a 2:1 compression ratio. The actual compression ratio may vary depending on the type of data being compressed.

**Table 1–4: Supported Formats for TLZn Tape Drives**

| Format | Device Special | Density Code | Compression | Capacity | Cartridge | I/O Supported |
|---|---|---|---|---|---|---|
| TLZ04 | rmt?a | 00h | N/A | 1.3 GB | DDS-1 (60m) | Read/Write |
| TLZ04 | rmt?l | 00h | N/A | 1.3 GB | DDS-1 60m) | Read/Write |
| TLZ04 | rmt?m | 00h | N/A | 1.3 GB | DDS-1 (60m) | Read/Write |
| TLZ04 | rmt?h | 00h | N/A | 1.3 GB | DDS-1 (60m) | Read/Write |
| TLZ06 | rmt?a | 00h | Off | 1.3 GB | DDS-1 (60m) | Read/Write |
| TLZ06 | rmt?l | 00h | Off | 1.3 GB | DDS-1 (60m) | Read/Write |
| TLZ06 | rmt?m | 00h | On | 2.6 GB * | DDS-1 (60m) | Read/Write |
| TLZ06 | rmt?h | 00h | On | 2.6 GB * | DDS-1 (60m) | Read/Write |
| TLZ06 | rmt?a | 00h | Off | 2.0 GB | DDS-1 (90m) | Read/Write |
| TLZ06 | rmt?l | 00h | Off | 2.0 GB | DDS-1 (90m) | Read/Write |
| TLZ06 | rmt?m | 00h | On | 4.0 GB * | DDS-1 (90m) | Read/Write |
| TLZ06 | rmt?h | 00h | On | 4.0 GB * | DDS-1 (90m) | Read/Write |
| TLZ07 | rmt?a | 00h | Off | 4.0 GB | DDS-2 | Read/Write |
| TLZ07 | rmt?l | 00h | Off | 4.0 GB | DDS-2 | Read/Write |
| TLZ07 | rmt?m | 00h | On | 8.0 GB * | DDS-2 | Read/Write |
| TLZ07 | rmt?h | 00h | On | 8.0 GB * | DDS-2 | Read/Write |
| TLZ09 | rmt?a | 00h | Off | 4.0 GB | DDS-2 | Read/Write |
| TLZ09 | rmt?l | 00h | Off | 4.0 GB | DDS-2 | Read/Write |
| TLZ09 | rmt?m | 00h | On | 8.0 GB * | DDS-2 | Read/Write |
| TLZ09 | rmt?h | 00h | On | 8.0 GB * | DDS-2 | Read/Write |
| TLZ10 | rmt?a | 00h | Off | 12.0 GB | DDS-3 | Read/Write |
| TLZ10 | rmt?l | 00h | Off | 12.0 GB | DDS-3 | Read/Write |
| TLZ10 | rmt?m | 00h | On | 24.0 GB * | DDS-3 | Read/Write |
| TLZ10 | rmt?h | 00h | On | 24.0 GB * | DDS-3 | Read/Write |

Table 1–5 provides information about TZS20 Tape Drives.

**Table 1–5: Supported Formats for TZS20 Tape Drives**

| Format | Device Special | Density Code | Compression | Capacity | Cartridge | I/O Supported |
|---|---|---|---|---|---|---|
| TZS20 | rmt?a | 00h | Off | 25.0 GB | AIT | Read/Write |
| TZS20 | rmt?l | 00h | Off | 25.0 GB | AIT | Read/Write |
| TZS20 | rmt?m | 00h | On | 50.0 GB * | AIT | Read/Write |
| TZS20 | rmt?h | 00h | On | 50.0 GB * | AIT | Read/Write |

# 2

# Summary of Available Server Environment Patches

This chapter summarizes the Available Server Environment patches included in Patch Kit-0005.

Table 2–1 lists patches that have been updated.

**Table 2–1: Updated Available Server Environment Patches**

| Patch IDs | Change Summary |
|---|---|
| Patch 20.00 | New |
| Patches 11.00, 5.00, 21.00 | Superseded by Patch 24.00 |
| Patches 4.00, 6.00, 7.00, 8.00, 13.00, 16.00, 17.00, 18.00, 22.00, 23.00 | Superseded by Patch 25.00 |
| Patches 4.00, 6.00, 7.00, 8.00, 13.00, 16.00, 17.00, 18.00, 22.00, 23.00 | Superseded by Patch 26.00 |
| Patches 2.00, 9.00 | Superseded by Patch 19.01 |

Table 2–2 provides a summary of patches in Patch Kit-0005.

**Table 2–2: Summary of Available Server Environment Patches**

| Patch IDs | Abstract |
|---|---|
| Patch 3.00<br>ASE130-003 | **Patch:** Cluster Map Creation Correction<br>**State:** Supersedes patch ASE130-001 (01.00)<br>This patch fixes the following problems:<br>• This problem occurs when an ASE site has defined ifconfig parameters beyond the the netmask in the /etc/rc.config file. When this occurs the cluster map cannot be created and the makeclmap program dumps core. This problem only affects ASE sites with 1.3.<br>• This patch fixes the problem of the cluster monitor not properly identifying all the HSZ40 devices in the cluster map. |
| Patch 10.00<br>ASE130-015 | **Patch:** Disk Label, Retry Command Correction<br>**State:** Existing<br>This patch fixes the following problems with Logical Storage Manager (LSM) volumes in a DECsafe Available Server Environment (ASE):<br>• After installing a patch to the LSM voldisk command, the disk labels of LSM disks are inadvertently being reinitialized during service modification. This causes attempts to start the service to fail and leaves the service unassigned.<br>• Certain LSM operations that should have been retried were failing on the first attempt.<br>• Retry messages were not being printed to the log file. |

**Table 2–2: Summary of Available Server Environment Patches (cont.)**

| | |
|---|---|
| Patch 12.00<br>ASE130-017 | **Patch:** Correction For Service Aliases<br>**State:** Existing<br>This patch fixes a problem in /var/opt/ASE130/ase/sbin/nfs_ifconfig that corrupts the memory resident routing table and subsequent netstat output (netstat -r) during ASE service failover. |
| Patch 15.00<br>ASE130-020 | **Patch:** Recognize KZPBA Correction<br>**State:** Existing<br>This patch adds KZPBA controller support for the ase_fix_config utility. |
| Patch 19.01<br>ASE130-024-1 | **Patch:** System Panic, SCSI Error Condition Correction<br>**State:** Supersedes patches ASE130-002 (02.00), ASE130-014 (09.00)<br>This patch fixes the following problems:<br>• Fixes the following problems in the ASE Availability Manager (AM):<br>– A "simple_lock: time limit exceeded" panic on multi-processor, and system hangs in single processor systems. This can occur when multiple host target mode requests are issued due to SCSI aborts and resets on a shared bus.<br>– A kernel memory fault panic caused by a race condition when the AM de-initializes.<br>• Fixes three problems in the Availability Manager:<br>– Kernel memory fault in am_select()<br>– Unit Attentions exhausting retries<br>– kernel memory fault in am_ping_complete()<br>• Fixes SCSI host ping drop out problem. This problem would occur 0 to 20 or more times a day with drop out periods of 30 seconds. The problem appears to only happen in ASE environments with three or more members. |
| Patch 20.00<br>ASE130-018 | **Patch:** ASE Service Correction<br>**State:** New<br>Running the vquotacheck command on a filesystem participating in an ASE service will cause a system to panic if the service fails over or relocates while the command is in progress. |
| Patch 24.00<br>ASE130-028 | **Patch:** ASE Data Base For LSM Correction<br>**State:** Supersedes patches ASE130-016 (11.00), ASE130-005 (5.00), ASE130-025 (21.00)<br>This patch fixes the following problems:<br>• Fixes a problem where changes in the LSM configuration were not being properly handled during the delete of an LSM volume from a service.<br>• Increases the timeout values for the LSM action scripts that are part of the TruCluster Production Server, Available Server and DECsafe Available Server products. The timeouts were too small for large LSM configurations and, under certain conditions, would cause the start of the services to fail, leaving them unassigned.<br>• DECsafe does not correctly support the removal of volumes from AdvFS domains that are assigned to ASE services.<br>• Fixes a problem in which under certain circumstances, an ASE service modification could result in a corrupted configuration data base. |

**Table 2–2: Summary of Available Server Environment Patches (cont.)**

| | |
|---|---|
| Patch 26.00<br>ASE130-027B | **Patch:** Not Properly Handling Error Condition Correction<br>**State:** Supersedes patches ASE130-004 (04.00), ASE130-011 (06.00), ASE130-012 (07.00), ASE130-013 (08.00), ASE130-019 (13.00), ASE130-021 (16.00), ASE130-022 (17.00), ASE130-023 (18.00), ASE130-026 (22.00), ASE130-027 (23.00)<br>This patch fixes the following problems:<br>• Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and Production Server software.<br>When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied:<br>msgSvc: message queue overflow, LOST MESSAGE!<br>From this point on, no further messages will be received.<br>• Fixes a problem that may occur in an ASE (either DECsafe ASE Version 1.3, TruCluster Available Server, or TruCluster Production Server) when the ASE encounters connection attempts from hosts whose IP addresses cannot be resolved to hostnames. Instead of printing a warning about a possible security breach, the ASE daemons will core dump with a segmentation violation. One cause of this problem may be unknown hosts on the network using public domain internet security software which scans all TCP ports on remote hosts.<br>• This patch is part of the set of DIGITAL UNIX patches required to support the HSZ70 UltraSCSI Raid Array controller on the KZPSA adapter under ASE 1.3.<br>• This patch corrects a problem whereby the ASE agent daemon (aseagent), ASE director daemon (asedirector), the trigger-action server daemon (tractd), or the submon process fails and exits without a core file if a SIGPIPE or other stray signal occurs.<br>• Pulling a network cable on all ASE members results in the asedirector exiting. Replacing the cable in any ASE member would not start a director.<br>The director restart logic in the agent was not starting a director in some cases that it should have been. All cases are now explicitly handled in this code. This fixed a number of director restart problems related to network cable pulls.<br>• Pulling all monitored network interface cables on the machine running the asedirector and a service can result in another machine starting a new director and starting the same service before it has been fully stopped on the first machine. This is especially noticeable when a service takes a long time to stop.<br>This patch causes the host status monitor (asehsm) to actively go out and learn current member states before responding to the director with member state information.<br>• Fixes problem where reports about the ASE environment observed via the Cluster Monitor program (cmon) may be missing or incomplete. |

**Table 2–2: Summary of Available Server Environment Patches (cont.)**

| | |
|---|---|
| Patch 26.00 continued | • Fixes a problem where the cluster monitor either will not come up or has incomplete, or obviously incorrect, cluster status information.<br><br>This problem occurs on systems running ASE where, because of a network disconnect, hundreds of error messages were being logged in the daemon.log file. This file contained very large numbers of ASE_INQ_SERVICE failed messages or other similar messages.<br><br>The /usr/sbin/submon daemon fills the log with hundreds or thousands of "ASE_INQ_SERVICES failed or hung up" messages following a disconnect by the ASE director.<br><br>• 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.<br><br>• Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. |

**Table 2–2: Summary of Available Server Environment Patches (cont.)**

| | |
|---|---|
| Patch 27.00<br>ASE130-031 | **Patch:** asemgr Core Dumps<br>**State:** Supersedes patches ASE130-004 (04.00), ASE130-011 (06.00), ASE130-012 (07.00), ASE130-013 (08.00), ASE130-019 (13.00), ASE130-021 (16.00), ASE130-022 (17.00), ASE130-023 (18.00), ASE130-026 (22.00), ASE130-027 (23.00), ASE130-027A (25.00)<br>This patch fixes the following problems:<br>• This patch corrects a problem in which the asemgr can core dump when adding a member back into an ASE.<br>• Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and Production Server software.<br>When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied:<br>msgSvc: message queue overflow, LOST MESSAGE!<br>From this point on, no further messages will be received.<br>• Fixes a problem that may occur in an ASE (either DECsafe ASE Version 1.3, TruCluster Available Server, or TruCluster Production Server) when the ASE encounters connection attempts from hosts whose IP addresses cannot be resolved to hostnames. Instead of printing a warning about a possible security breach, the ASE daemons will core dump with a segmentation violation. One cause of this problem may be unknown hosts on the network using public domain internet security software which scans all TCP ports on remote hosts.<br>• This patch is part of the set of DIGITAL UNIX patches required to support the HSZ70 UltraSCSI Raid Array controller on the KZPSA adapter under ASE 1.3.<br>• This patch corrects a problem whereby the ASE agent daemon (aseagent), ASE director daemon (asedirector), the trigger-action server daemon (tractd), or the submon process fails and exits without a core file if a SIGPIPE or other stray signal occurs.<br>• Pulling a network cable on all ASE members results in the asedirector exiting. Replacing the cable in any ASE member would not start a director.<br>The director restart logic in the agent was not starting a director in some cases that it should have been. All cases are now explicitly handled in this code. This fixed a number of director restart problems related to network cable pulls.<br>• Pulling all monitored network interface cables on the machine running the asedirector and a service can result in another machine starting a new director and starting the same service before it has been fully stopped on the first machine. This is especially noticeable when a service takes a long time to stop.<br>This patch causes the host status monitor (asehsm) to actively go out and learn current member states before responding to the director with member state information.<br>• Fixes problem where reports about the ASE environment observed via the Cluster Monitor program (cmon) may be missing or incomplete. |

**Table 2–2: Summary of Available Server Environment Patches (cont.)**

| | |
|---|---|
| Patch 27.00 continued | • Fixes a problem where the cluster monitor either will not come up or has incomplete, or obviously incorrect, cluster status information.<br><br>This problem occurs on systems running ASE where, because of a network disconnect, hundreds of error messages were being logged in the daemon.log file. This file contained very large numbers of ASE_INQ_SERVICE failed messages or other similar messages.<br><br>The /usr/sbin/submon daemon fills the log with hundreds or thousands of "ASE_INQ_SERVICES failed or hung up" messages following a disconnect by the ASE director.<br><br>• 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.<br><br>• Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. |

# 3

# Summary of Base Operating System Patches

This chapter summarizes the base operating system patches included in Patch Kit-0005.

Table 3–1 lists patches that have been updated.

Table 3–2 provides a summary of patches in Patch Kit-0005.

**Table 3–1: Updated Base Operating System Summary**

| Patch IDs | Change Summary |
|---|---|
| Patches 25.00, 253.00, 256.00, 265.00, 267.00, 307.00, 309.00, 310.00, 325.00, 332.00, 336.00, 342.00, 365.00, 368.00, 370.00, 375.00, 376.00, 378.00, 379.00, 383.00, 384.00, 387.00, 389.00, 390.00, 391.00, 398.00, 400.00, 402.00, 404.00, 409.00, 410.00, 412.00, 413.00, 420.00 | New |
| Patch 164.00 | Superseded by Patch 237.00 |
| Patch 41.00 | Superseded by Patch 255.00 |
| Patch 151.00 | Superseded by Patch 258.00 |
| Patches 148.00, 203.00, 205.00 | Superseded by Patch 263.00 |
| Patches 200.00, 183.00 | Superseded by Patch 266.00 |
| Patches 138.00, 158.00, 293.00 | Superseded by Patch 295.00 |
| Patch 63.00 | Superseded by Patch 298.00 |
| Patches 188.00, 271.00 | Superseded by Patch 302.00 |
| Patch 61.00 | Superseded by Patch 304.00 |
| Patches 58.00, 252.00 | Superseded by Patch 308.00 |
| Patches 282.00, 317.00 | Superseded by Patch 327.00 |
| Patch 222.00 | Superseded by Patch 329.00 |
| Patches 84.00, 229.00, 289.00, 82.00, 322.00 | Superseded by Patch 364.00 |
| Patch 221.00 | Superseded by Patch 371.00 |
| Patches 93.00, 95.00, 101.00, 114.00, 126.00, 81.00, 180.00, 244.00, 268.00, 280.00, 2.00, 239.00, 83.00, 251.00, 259.00, 260.00, 321.00, 415.00 | Superseded by Patch 372.00 |
| Patch104.00 | Superseded by Patch 374.00 |
| Patches 47.00, 77.00, 80.00, 52.00, 85.00, 87.00, 153.00, 197.00, 198.00, 217.00, 288.00, 172.00, 264.00, 294.00, 299.00, 314.00, 324.00, 331.00, 333.00, 361.00, 362.00, 363.00, 369.00, 411.00 | Superseded by Patch 380.00 |
| Patches 99.00, 133.00, 335.00, 25400 | Superseded by Patch 381.00 |
| Patches 65.00, 68.00, 191.00, 192.00, 145.00, 214.00, 71.00, 246.00, 285.00, 248.00, 261.00, 311.00, 330.00 | Superseded by Patch 386.00 |
| Patch 181.00 | Superseded by Patch 397.00 |

**Table 3–1: Updated Base Operating System Summary (cont.)**

| | |
|---|---|
| Patches 70.00, 202.00, 202.01, 234.00, 326.00, 346.00 | Superseded by Patch 401.00 |
| Patch 241.00 | Superseded by Patch 405.00 |
| Patches 245.00, 219.00, 170.00, 300.00, 313.00, 403.00 | Superseded by Patch 406.00 |
| Patches 115.00, 154.01 | Superseded by Patch 407.00 |
| Patches 75.00, 79.00, 49.00), 50.00, 56.00, 275.00, 249.00, 297.00, 301.00, 318.00, 334.00, 366.00, 395.00 | Superseded by Patch 408.00 |
| Patches 184.00. 303.00 | Superseded by Patch 414.00 |
| Patches 55.00, 86.00, 86.01, 86.02, 89.00, 89.01, 187.00, 243.00, 196.00, 207.00, 204.00, 206.00, 230.00, 242.00, 286.00, 287.00, 279.00, 283.00, 292.00, 306.00, 319.00, 320.00, 392.00, 396.00 | Superseded by Patch 417.00 |
| Patches 64.00, 69.00, 113.00, 149.00, 228.00, 273.00, 276.00, 53.00, 62.00, 236.00, 262.00, 305.00, 315.00, 328.00 | Superseded by Patch 418.00 |
| Patches 194.00, 90.00, 388.00, 399.00 | Superseded by Patch 419.00 |
| Patch 117.00 | Superseded by Patch 422.00 |
| Patch 96.00 | Superseded by Patch 424.00 |
| Patch 96.00 | Superseded by Patch 425.00 |
| Patches 107.00, 108.00 | Superseded by Patch 426.00 |
| Patches 107.00, 108.00 | Superseded by Patch 427.00 |
| Patch 21.00 | Superseded by Patch 428.00 |
| Patch 211.00 | Superseded by Patch 429.00 |

**Table 3–2: Summary of Base Operating System Patches**

| Patch IDs | Abstract |
|---|---|
| Patch 59.00<br>OSF375-059 | **Patch:** fddi_config Fails Attempt To Config The fta Device<br>**State:** Existing<br>The fddi_config program was not shipped with the V3.2G kit. Unfortunately, the fddi_config from previous versions fails when attempting to config the fta device. Applying this file solves the problem. |
| Patch 67.00<br>OSF375-370040 | **Patch:** NCR psiop Driver Correction<br>**State:** Existing<br>This patch fixes a problem that occurs with the NCR 53C8XX driver (psiop) which the device may not appear to be on the SCSI bus. |
| Patch 92.00<br>OSF375-350216 | **Patch:** volrecover -b Command Correction<br>**State:** Existing<br>This patch fixes a problem that occurs when the -b option of the volrecover command is used. The problem is that a background job spawned to perform the recovery operation fails when a SIGHUP signal is received. |
| Patch 94.00<br>OSF375-350221 | **Patch:** mfa Driver Correction<br>**State:** Existing<br>This patch fixes a halt/restart problem with the mfa driver ESP self-test. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 97.00<br>OSF375-350231 | **Patch:** System V getdirentries() System Call Error<br>**State:** Existing<br>The System V getdirentries() system call did not correctly calculate the number of entries in a directory inode when accessing the /dev/fd file system. |
| Patch 102.00<br>OSF375-350237 | **Patch:** find Command Correction<br>**State:** Existing<br>The find command will not handle more than 100 arguments. |
| Patch 103.00<br>OSF375-350238 | **Patch:** Mail Sent Using uucp or Output Using uux Error<br>**State:** Existing<br>Mail sent using uucp, or output to Mail from the uux command causes the mail message to be sent from the daemon to root with the following error message: "remote access to path/file denied". The error message is sent to root in a mail message. |
| Patch 105.00<br>OSF375-350240 | **Patch:** showmount -e Command Correction<br>**State:** Existing<br>Add the time out options -t nnn & -T to the 'showmount' command. |
| Patch 106.00<br>OSF375-350241 | **Patch:** Incorrect Profiling Data<br>**State:** Existing<br>This patch corrects the following:<br>• Fixes a problem that occurs on a multiprocessor system in which the pfm driver does not provide any profiling data on CPUs other than #0.<br>• Fixes a problem that occurs on systems with recent CPU hardware (EV5) in which using the kprofile command will cause the system to hang. |
| Patch 111.01<br>OSF375-350249-1 | **Patch:** Kernel LMF Corrections<br>**State:** Existing<br>Permits kernel components to release license units that have been allocated through lmf_auth_ex(). |
| Patch 112.00<br>OSF375-350251 | **Patch:** Kernel Memory Fault Panic (bcopy) Correction<br>**State:** Existing<br>System panics with a kernel memory fault in k_mem_fault. |
| Patch 118.00<br>OSF375-350263 | **Patch:** Mail From "daemon" Not Sender Correction<br>**State:** Existing<br>Mail from non-local senders appears to be from "daemon" rather than the person who originated the mail. |
| Patch 120.00<br>OSF375-350268 | **Patch:** mkpasswd Command Correction<br>**State:** Existing<br>This patch fixes a problem with the mkpasswd command. Hashed password database files (for example, /etc/passwd.pag and /etc/passwd.dir) are deleted before new database files are created. |
| Patch 121.00<br>OSF375-350269 | **Patch:** Process Hang On SMP System<br>**State:** Existing<br>Calls to flock() can hang a process on an SMP system if 2 or more processes are attempting to obtain and release an flock() on the same file. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 122.00<br>OSF375-370036 | **Patch:** Prevent SMP System Duplicate namecache Entries<br>**State:** Existing<br>Problem in DIGITAL UNIX SMP systems where duplicate namecache entries are being created and if heavy file system lookup operations may eventually result in a simple lock timeout and a system panic. |
| Patch 123.00<br>OSF375-350273 | **Patch:** rmt Program Correction<br>**State:** Existing<br>This patch fixes a problem that occurs when using the rmt program to access devices or files. The rmt program does not accept reads/writes of less than 1024 bytes. The system displays the following error message:<br><br>Cannot set socket receive buffer size |
| Patch 124.01<br>OSF375-350275-1 | **Patch:** rlogin Correction<br>**State:** Existing<br>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. DIGITAL has corrected this potential vulnerability. |
| Patch 125.00<br>OSF375-350278 | **Patch:** dump/rdump Command Corrections<br>**State:** Existing<br>This patch fixes a problem in dump and rdump. When the -n flag was used, an extraneous file (/dev/:0) was sometimes being created. |
| Patch 127.00<br>OSF375-350284 | **Patch:** Asian atty Correction<br>**State:** Existing<br>This patch corrects a problem where a remote user will kill rlogin or telnet and the server host will have an orphaned login process and rlogind or telnetd process in sleep state indefinitely. This is seen only with Asian tty (atty) or any other host which is running c-list rather than STREAMS tty's. |
| Patch 128.00<br>OSF375-350285 | **Patch:** more Command Correction<br>**State:** Existing<br>Rectified erroneous behavior of 'more' command when displaying files generated by Oracle. |
| Patch 129.00<br>OSF375-350286 | **Patch:** Funnelled Non-Timeshared Thread Correction<br>**State:** Existing<br>This patch fixes a deadlock problem that may occur when a non-timeshared thread becomes funnelled. |
| Patch 130.00<br>OSF375-350287 | **Patch:** Correction For floating-point exception<br>**State:** Existing<br>This patch fixes a problem that causes some valid programs compiled with IEEE mode to receive a floating-point exception even though they should run to completion. |
| Patch 132.00<br>OSF375-350289 | **Patch:** Compiler Incorrect Codegen Sequence Correction<br>**State:** Existing<br>The code generator used an incorrect codegen sequence when doing stack allocation within procedure prologs where the size of the stack was very large (for example, when a structure is passed as an entity rather than as a pointer). |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 134.00<br>OSF375-350293 | **Patch:** LAT Correction<br>**State:** Existing<br>This patch corrects a problem where processes such as wall, ntalkd, and comsat, when associated with LAT devices, get stuck in the 'u' state (processes are hung) and cannot be cleared from the system. |
| Patch 136.00<br>OSF375-350297 | **Patch:** Corrections For Symbolic Link To Root File System<br>**State:** Existing<br>Fixes a problem that causes the system to panic after creating a symbolic link to the root file system ('/') and accessing it like a normal file. |
| Patch 137.00<br>OSF375-350298 | **Patch:** Security, (SSRT0362U)<br>**State:** Supersedes patches OSF375-350267 (119.00), OSF375-350267-1 (119.01)<br>This patch corrects the following:<br>• On systems running enhanced security, the login process may fail with a segmentation fault.<br>• A security vulnerability has been discovered when running enhanced security that may facilitate unauthorized users gaining access to the system. DIGITAL has corrected this vulnerability. |
| Patch 139.00<br>OSF375-350301 | **Patch:** ping Command Correction<br>**State:** Existing<br>This patch fixes a problem in which the ping command can time out after invoking the "rcinet restart" command. |
| Patch 143.00<br>OSF375-350306 | **Patch:** Certain Keyboards Stop Functioning After Logout<br>**State:** Supersedes patch OSF375-350245 (109.00)<br>This patch corrects the following:<br>• On systems with PCXAL, LK411, and similar keyboards, sometimes the keyboard stops working.<br>• On systems with PCXAL, LK411, and similar keyboards, after logging out of a session on the workstation monitor, sometimes the keyboard stops working. A reboot is required to clear the problem. |
| Patch 144.00<br>OSF375-350308 | **Patch:** ATM Correction<br>**State:** Existing<br>This patch prevents a panic that can occur after deleting an ATM ARP entry. The user command to delete an ATM ARP entry is "atmarp -d". Subsequent access to the ATM ARP table can cause the panic. |
| Patch 147.00<br>OSF375-350313 | **Patch:** Kernel Memory Fault Panic (svc_auth_unix) Correction<br>**State:** Existing<br>This patch fixes a problem that occurs when the system panics with the following error message:<br>`kernel memory fault` |
| Patch 150.00<br>OSF375-350317 | **Patch:** select() Missing State Change Correction<br>**State:** Existing<br>This patch fixes a network socket problem with select() missing state changes on clients from non-write to writable. |
| Patch 152.00<br>OSF375-350322 | **Patch:** OSF375-350322<br>**State:** Existing<br>This patch fixes a problem where telnet dumps core if the USER environment variable is the last variable in the environment list. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 157.00<br>OSF375-350334 | **Patch:** EISA Corrections<br>**State:** Existing<br>This patch fixes two problems that occur on systems with an EISA bus:<br>• A system running four DE425 adapters off an EISA bus may hang.<br>• If a device's EISA configuration file contains a function DISABLE keyword and the DISABLE option is selected, the device's driver may not be configured and probed at bus configuration time. |
| Patch 159.00<br>OSF375-350336 | **Patch:** Multithreaded Apps Hang On SMP Systems Correction<br>**State:** Existing<br>This patch corrects a problem where multithreaded applications will experience a hang on SMP systems. |
| Patch 162.00<br>OSF375X-350019 | **Patch:** User Not Added To New Group<br>**State:** Existing<br>This patch fixes the following problem: If the customer adds a new group with XSysAdmin and then tries to use XIsso to add the user into the new group, the group shows up but the user never gets added. |
| Patch 163.00<br>OSF375X-350020 | **Patch:** Slow X Server Performance Drawing Arcs<br>**State:** Existing<br>X server performance is slow when an application is drawing arcs which are outside the bounds of the drawable window. |
| Patch 165.00<br>OSF375-350351 | **Patch:** Security, talkd (SSRT0446U)<br>**State:** Existing<br>A potential security vulnerability has been discovered in talkd, where under certain circumstances, system integrity may be compromised. DIGITAL has corrected this potential vulnerability. |
| Patch 166.00<br>OSF375X-350023 | **Patch:** dxterm Support To Suppress ANSI Escape Sequences<br>**State:** Existing<br>This patch adds the new resource printOnlyPrintables to dxterm. When this resource is set to TRUE (the default is FALSE), dxterm will not output any escape sequences when printing. This is needed for some PostScript printer (filters) that can not handle escape sequences. |
| Patch 167.00<br>OSF375X-350038 | **Patch:** Corrects Memory Leak In The Motif Text Widgets<br>**State:** Supersedes patch OSF375X-350035 (201.00)<br>This patch corrects the following:<br>• Motif Text widget is afflicted with a memory leak. A small amount of dynamic memory is lost each time the background colors in the widget are changed.<br>• Motif applications may abort when you use the drag-and-drop feature. |
| Patch 168.00<br>OSF375X-350025 | **Patch:** Bookreader Hang Correction<br>**State:** Existing<br>Bookreader hangs when displaying certain pages if the required fonts are not available. This problem usually occurs when redirecting Bookreader's display to another vendor's workstation (HP or Sun). |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 173.01<br>OSF375-360082B-1 | **Patch:** named, screend Corrections<br>**State:** Existing<br>A potential security vulnerability has been discovered in bind, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. |
| Patch 174.01<br>OSF375-360082C-1 | **Patch:** uucp Command Corrections<br>**State:** Existing<br>A potential security vulnerability has been discovered in bind, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. |
| Patch 178.00<br>OSF375-350345 | **Patch:** UFS 32GB File write Performance Correction<br>**State:** Existing<br>Data written to a file greater than 32 GB in length will be slower than data written to the file when it is less than 32 GB in length. |
| Patch 179.00<br>OSF375-360081 | **Patch:** getty Command Option Correction<br>**State:** Existing<br>Allows getty to accept uppercase usernames. |
| Patch 185.00<br>OSF375-350362 | **Patch:** mailx Command Corrections<br>**State:** Existing<br>Fixes an error that occurs when replying to a message in which the "CC:" field contains blank-separated names not enclosed in angle brackets ("<...>"). |
| Patch 190.00<br>OSF375-067 | **Patch:** Potential Data-Corrupt, DE500-AA e-net Adapt<br>**State:** Supersedes patch OSF375-048 (48.00), OSF375-066 (189.00)<br>This patch corrects the following:<br>• Upgrade/replacement for the ethernet driver when a DE500-AA, containing the DECchip 21140-AC, Fast Ethernet interface is used; allow filtering of greater than 16 multicast addresses and fixes the previous limitations to Hash/Perfect mode filtering.<br>• Fixes system panics on an SMP system with a tu (Tulip) Ethernet interface with the error message:<br>"System Uncorrectable Machine Check 660 (retry set)"<br>• Driver workaround to avoid potential data-corruption problem inherent in the DE500-AA 10/100 Mbps Ethernet adapter. |
| Patch 193.00<br>OSF375-350247 | **Patch:** acctcom Command Correction<br>**State:** Existing<br>Fixes a problem in which the size field of a process displayed by the acctcom command is displayed incorrectly. |
| Patch 199.00<br>OSF375X-350033 | **Patch:** dxsession Close Button Operation Correction<br>**State:** Existing<br>Fixes problem where exiting from the DECwindows Session Manager (dxsession) via the 'Close' option of the window menu results in an undesirable saving of dxsession's scratch file in /tmp. Use of this button also causes a behavior inconsistent, with dxsession's 'End Session' button. |
| Patch 209.00<br>OSF375-360095 | **Patch:** telnetd Correction<br>**State:** Existing<br>Prevents a long delay while trying to log out using telnet. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 210.00<br>OSF375-370057 | **Patch:** Kernel Builds But Is Not Bootable<br>**State:** Existing<br>Fixes a problem that occurs on AlphaServer 4100 systems in which the kernel will build, but is not bootable. |
| Patch 212.00<br>OSF375-360097 | **Patch:** Misc nfs_client Problems<br>**State:** Existing<br>Fixes a problem in which the system crashes when attempting to NFS mount a text file. |
| Patch 213.00<br>OSF375-360098 | **Patch:** Pipe Function Correction<br>**State:** Existing<br>Fixes a problem in which the system crashes when attempting to NFS mount a text file. |
| Patch 218.00<br>OSF375X-005 | **Patch:** Issues With S3 Trio64/ATI Mach64 Graphics Cards<br>**State:** Supersedes patch OSF375X-365003 (161.00), OSF375X-350032 (175.00)<br>This patch corrects the following:<br>• On systems with an S3 Trio64V+ graphics card (PB2GA-JC or PB2GA-JD), the X server hangs while drawing the login screen.<br>• Systems with an S3 Trio64 graphics card can loose time (on the order of a few minutes a day).<br>• On systems with an ATI Mach64 graphics card, sometimes the monitor will lose synchronization or become stuck in power-save mode. |
| Patch 220.00<br>OSF375-350384 | **Patch:** Various Sckt, Net, pcktfltr, panic Corrections<br>**State:** Supersedes patches OSF375-350248 (110.00), OSF375-350294 (135.00), OSF375-350305 (142.00), OSF375-350342 (177.00), OSF375-365055 (208.00), OSF375-365057 (233.00)<br>This patch corrects the following:<br>• Enhanced fix to the solockpair() routine; problem symptoms include kernel memory faults with sockets, mbufs and mblocks as well as hangs. Applications using sockets in a multi-threaded, multi-cpu environment can experience a number of lock violations with the socket structures.<br>• Fixes a problem in which packet filter programs do not receive packets when the source is sending multicast packets on an Ethernet network.<br>• Fixes a problem in which network applications communicating to one of the host's own addresses, may hang, or receive the error message:<br>no buffer space available<br>• Fixes situation of a DIGITAL UNIX system connected to a token ring network receiving a ping, not being able to respond and the token ring driver displays "List Error in transmit" message.<br>• A "panic: lock_read: hierarchy violation in del_dealloc_stg" error occurs when a socket lock is held by a UNIX domain while calling vrele().<br>• Fixes a system panic caused by a Windows95 or WindowsNT system sending an illegal length ping (ICMP) packet.<br>• Fixes a kernel memory fault panic that occurs on SMP platforms when running the Unicenter product from Computer Associates in conjunction with Oracle software. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00<br>OSF375-350405 | **Patch:** SMP "simple_lock: time limit exceeded" Correction<br>**State:** Existing<br>Fixes panics that may occur on SMP systems with message:<br>"simple_lock: time limit exceeded" |
| Patch 226.00<br>OSF375-350407 | **Patch:** Device Driver Corrections<br>**State:** Supersedes patch OSF375-350363 (186.00)<br>This patch corrects the following:<br>• Fixes a problem in which a system with an HSZ70 controller with a Q-Logic adapter or a KZPSA adapter may experience kernel memory faults during a failover and display a message similar to the following:<br>panic (cpu 8): kernel memory fault<br>cam_logger: CAM_ERROR entry too large to log!<br>• A custom SCSI driver may return the error ENOMEM from its ccmn_open_unit() routine. |
| Patch 227.00<br>OSF375-350410 | **Patch:** File System Incorrect User Type Correction<br>**State:** Existing<br>Fixes a problem that causes an AdvFS file system encapsulated under LSM to appear as a user type of "gen", rather than the correct type, "fsgen". |
| Patch 231.00<br>OSF375-360109 | **Patch:** "simple lock time limit exceeded" System Panic<br>**State:** Existing<br>Fixes a problem that occurs on SMP systems using LSM in which the system panics with a "simple lock time limit exceeded" message. |
| Patch 235.00<br>OSF375-370055 | **Patch:** Kernel Memory Faults During Booting<br>**State:** Existing<br>Fixes a problem where an AlphaServer 4100 may panic with a kernel memory fault where a system has more than 32 Mb of memory and the console variable MEMORY_TEST is set to "partial". |
| Patch 237.00<br>OSF375X-006 | **Patch:** Bookreader UID Handling Correction<br>**State:** Supersedes patch OSF375X-350037 (164.00)<br>• Fixes a problem in which a Bookreader library routine does not restore the effective UID.<br>• When called from an application, bookreader changes the caller's effective UID to the real UID, but then never restores it to the original effective UID, before returning control to the calling program. |
| Patch 238.00<br>OSF375-084 | **Patch:** System Will Not Reboot, System Crash Booting<br>**State:** Supersedes patch OSF375-057 (57.00)<br>This patch corrects the following:<br>• Fixes problem on AlphaServer 2100A system; when the system is shut down using the "shutdown -r" command, the system will not reboot.<br>• Alphaserver 2100A system crashes during boot with greater than 1GB of memory installed. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 247.00<br>OSF375-093 | **Patch:** ar Command Corrections<br>**State:** Supersedes patch OSF375-060 (60.00)<br>This patch corrects the following:<br>• The ar command is unable to find object modules specified for deletion or extraction whose names are longer than 13 characters.<br>• This patch fixes a problem with the ar command's -x option, which extracts archive files. Without this fix, the ar command's -x option may, in error, return a message stating that the specified archive file was not found. |
| Patch 250.00<br>OSF375-100 | **Patch:** who Command Correction<br>**State:** New<br>Corrects a problem that occurs when more than 140 users are logged on to a system and the who command is issued. If the output from the command is redirected or piped, the last several lines become corrupt. |
| Patch 253.00<br>OSF375-104 | **Patch:** rdist Utility Correction<br>**State:** New<br>Correction for rdist Utility to prevent segmentation fault. |
| Patch 255.00<br>OSF375-106 | **Patch:** rpc.statd Daemon Corrections, Security (SSRT0456U)<br>**State:** Supersedes patch OSF375-350304 (141.00)<br>This patch corrects the following:<br>• 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. DIGITAL has corrected this potential vulnerability.<br>• Fixes a problem that occurs in ASE/TCR environments in which the rpc.statd daemon does not start when using the -p option to specify a long pathname (> 45 characters). When this happens, NFS locking to the NFS service fails causing applications like mail to hang. |
| Patch 256.00<br>OSF375-107 | **Patch:** Security, restore (SSRT0490U)<br>**State:** New<br>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. DIGITAL has corrected this potential vulnerability. |
| Patch 258.00<br>OSF375-109 | **Patch:** ftp Command Correction, Security (SSRT0505U)<br>**State:** Supersedes patch OSF375-350318 (151.00)<br>This patch corrects the following:<br>• 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. DIGITAL has corrected this potential vulnerability.<br>• This patch fixes a problem with the ftp command. If you ftp to an IBM MVS system using the IP address, the IBM system will refuse the connection. This problem can be encountered on any system that validates TOS (Type Of Service) requests if the file /etc/iptos is not used on the client. It is recommended that this patch be installed on all OSF systems. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 263.00<br>OSF375-114 | **Patch:** Library Corrections<br>**State:** Supersedes patch OSF375-350315 (148.00), OSF375-350368 (203.00), OSF375-350374 (205.00)<br>This patch corrects the following:<br>• Resolves a hang in the xticlose() routine and a kernel memory fault in the xti_discon_req() routine.<br>• Fixes a problem for TLI applications which make use of the t_accept library routine. The secondary endpoint state is not being set correctly.<br>• Corrects a problem encountered by tli applications which do an abort disconnect on an endpoint which was established as an orderly release endpoint and leave the endpoint in an unexpected state.<br>• Ensures that t_errno is set even when trcv retrieves no data. |
| Patch 265.00<br>OSF375-116 | **Patch:** Kernel Memory Fault Panic Correction<br>**State:** New<br>Corrects a problem that occurs on Alpha VME 4/2xx systems. The system may panic and display the following error message:<br>kernel access memory fault |
| Patch 266.00<br>OSF375-117 | **Patch:** Correction For ufs_fsck, fsck, Prop List Corr<br>**State:** Supersedes patches OSF375-350347 (200.00), OSF375-350357 (183.00)<br>This patch corrects the following:<br>• Fixes a ufs_fsck problem where ufs_fsck would mishandle certain dir corruptions, recursively asking the user if they want to fix it.<br>• Fixes fsck operation where if fsck is run on a non-existent file system or on a currently mounted file system, it returns a success status of zero. It should return a non-zero status.<br>• Fixes a problem in which the UFS property list can become corrupted. |
| Patch 267.00<br>OSF375-118 | **Patch:** Corrects Several pcnfsd Problems<br>**State:** New<br>This patch corrects the following:<br>• Printing from a PC via pcnfsd and logged in as user nobody would report a "file not found" or "access violation" error message.<br>• When signals causing pcnfsd to terminate or when a SIGPIPE signal was not caught, pcnfsd would exit without producing a core file.<br>• The pcnfsd authentication would cause crashes and memory corruption. |
| Patch 269.00<br>OSF375-350413 | **Patch:** audit_tool Command Correction<br>**State:** Existing<br>The audit_tool command hangs if the audit log contains pathnames that encounter boundary conditions. |
| Patch 270.00<br>OSF375-350418 | **Patch:** awk Command Correction<br>**State:** Existing<br>awk consumes memory until the machine swaps itself and core dumps with:<br>write failed, file system is full  Memory fault - core dumped |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 272.00<br>OSF375-350420 | **Patch:** Security, mountd (SSRT0496U)<br>**State:** Existing<br>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. DIGITAL has corrected this potential vulnerability. |
| Patch 274.00<br>OSF375-350423 | **Patch:** doconfig Hang Correction<br>**State:** Existing<br>Fixes a problem the doconfig program hangs after being invoked by the uuxqt program. |
| Patch 277.00<br>OSF375-350443 | **Patch:** Linker Corrections<br>**State:** Supersedes patches OSF375-360049 (78.00), OSF375-360073 (88.00), OSF375-350337 (160.00)<br>This patch corrects the following:<br>• Fixes the following linker problems:<br>– Hidden/export symbol wildcard problem<br>– Assert getting generated with R_GPVALUE relocations<br>– Improper Text segment alignment processing<br>– Internal memory managment problem processing C++ program<br>• This patch fixes a problem where use of "ld -r" will change symbol preemption behavior.<br>• This patch changes how the linker handles permission problems with chmod(), boundary check for OMAGIC (impure) object files.<br>• This patch fixes a performance problem that the linker has with hidden symbols (-hidden flag) and large numbers of shared library files (.so files). |
| Patch 278.00<br>OSF375-350445 | **Patch:** Out Of Order Packets, Mem Leak Corrections<br>**State:** Supersedes patch OSF375-350288 (131.00)<br>This patch corrects the following:<br>• Fixes a memory leak problem using the STREAMS Data Link Bridge (dlb) pseudodevice driver and could cause a "freeing free mbuf" panic when system memory is exhausted.<br>• This patch corrects a problem with packets out of order experienced by some PATHWORKS Netbuei clients. |
| Patch 281.00<br>OSF375-350452 | **Patch:** "advfsstat -n" Causes A Core Dump<br>**State:** Existing<br>Fixes an AdvFS problem in which the "advfsstat -n" command causes a core dump. The system displays the message:<br>Memory fault(coredump) |
| Patch 284.00<br>OSF375-370059 | **Patch:** io_zero() System Call Returns An Incorrect Value<br>**State:** Existing<br>Fixes a problem in which the io_zero() system call returns an incorrect value on an AlphaServer 1000. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 290.00<br>OSF375-360116 | **Patch:** "vquotacheck -a" Erroneously Sets Quotas<br>**State:** Existing<br>Fixes a problem where the AdvFS filesystem command "vquotacheck -a" erroneously sets all quotas for users to values derived from the last AdvFS fileset in /etc/fstab, rather than the correct values for each individual fileset. |
| Patch 291.00<br>OSF375-350213 | **Patch:** LSM Volumes Remain in SYNC State<br>**State:** Existing<br>Fixes a problem on ASE systems where LSM volumes remain in SYNC state when no volume resync or volplex att command is running. This results in performance degradation. |
| Patch 295.00<br>OSF375-123 | **Patch:** Security, ftpd (SSRT0448U, SSRT0452U)<br>**State:** Supersedes patches OSF375-350300 (138.00), OSF375-350335 (158.00), OSF375-121 (293.00)<br>This patch corrects the following:<br>• 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. DIGITAL has corrected this potential vulnerability.<br>• When a user incorrectly logs in using the ftpd command, a "Login incorrect" message is displayed and after ftpd exits, the system will core dump.<br>• ftpd core dumps when using anonymous ftp with the ls commmand. |
| Patch 296.00<br>OSF375-124 | **Patch:** pax, cpio, tar Command Corrections<br>**State:** Supersedes patches OSF375-350303 (140.00), OSF375-350333 (156.00), OSF375-350333-1 (156.01), OSF375-350400 (223.00), OSF375-108 (257.00)<br>This patch corrects the following:<br>• Fixes the following problems with the pax command when cpio format is used:<br>– The cpio -z command hangs the system when small files are read using a large block size.<br>– When reading a series of commands, cpio fails on the second command and displays a "No input" error message. If an identical third cpio read is issued, cpio works as expected.<br>• Fixes a problem where the tar and pax programs incorrectly append files to an existing archive and cause the file to become corrupt.<br>• Fixes a problem with the tar "tv" command in reporting ownership on a file that had no legitimate owner at the time it was archived. Based on the position of the file in the archive, tar returned the owner of a previous file, or the values -973 for userid and -993 for groupid.<br>• Fixes pax's tar and cpio archive handling to allow filesizes greater than 4GB.<br>• The tar(pax) command doesn't correctly handle sparse files, especially Oracle database files. Pre-allocated space is not replaced on restore. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 298.00<br>OSF375-126 | **Patch:** Kernel Memory Faults, ICMP REDIRECTS Correction<br>**State:** Supersedes patch OSF375-063 (63.00)<br>This patch corrects the following:<br>• Fixes kernel memory faults in networking code from RTFREE.<br>• This patch fixes ICMP REDIRECTS. When an ICMP REDIRECT is received, the routing table was updated properly, but the IP layer didn't use the new route information. |
| Patch 302.00<br>OSF375-131 | **Patch:** FDDI Driver Corrections<br>**State:** Supersedes patches OSF375-350367 (188.00), OSF375-350419 (271.00)<br>This patch corrects the following:<br>• Fixes a kernel memory fault caused by the fta FDDI driver.<br>• Fixes a problem where after a hang the system crashes with the panic message: apecs_read_io_port. At that time, the only way to reboot the system is to switch it OFF then ON.<br>• Upgrade/Replacement for the "FTA" FDDI driver and fixes a DMA Error which can occur with the older driver. |
| Patch 304.00<br>OSF375-133 | **Patch:** network sockets Left In FIN_WAIT_1 State Correction<br>**State:** Supersedes patch OSF375-061 (61.00)<br>This patch corrects the following:<br>• Fixes a problem of memory corruption. A TCP control structure is illegally accessed after it is released. The corrupted memory buckets are the 256-byte size.<br>• This patch is a kernel fix for network sockets left in FIN_WAIT_1 state forever. This patch contains a "tunable" kernel parameter. It is recommended that only experienced system administrators attempt to set this parameter from the default value. |
| Patch 307.00<br>OSF375-136 | **Patch:** Corrects Printing To Console During A Panic<br>**State:** New<br>Corrects a problem for several platforms that don't print to the console terminal during a panic correctly. The particular platforms involved are AlphaStation 600, AlphaPC 164, AlphaServer 1000A 5/XXX, AlphaServer 1000 5/XXX, AXPvme 100 SBC, and DIGITAL Personal Workstation 433au, 500au, 600au. |
| Patch 308.00<br>OSF375-138 | **Patch:** Token Ring Driver Correction<br>**State:** Supersedes patch OSF375-058 (58.00), OSF375-103 (252.00)<br>This patch corrects the following:<br>• Upgrade/replacement for the Token Ring driver: fixes an intermittent kernel memory fault problem and additional enhancements added to transmit and receive list processing routines to ensure data integrity.<br>• This patch fixes a Token Ring transmission timeout. The driver can experience "ID 380PCI20001 (8/13/95)" as described in the TI380PCI Errata. |
| Patch 309.00<br>OSF375-139 | **Patch:** Corrects file-on-file System mount Panic<br>**State:** New<br>Corrects a problem in which a file-on-file system mount of either an NFS or a /proc file system will panic the system. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 310.00<br>OSF375-140 | **Patch:** Corrects lpd daemon Start Problem<br>**State:** New<br>Corrects a problem with the lpd line printer daemon when "/sbin/init.d/lpd stop" is followed right away by "/sbin/init.d/lpd start", the new lpd fails to start. The error message from syslog is:<br>/usr/spool/lpd.lock: locking failed: Operation would block |
| Patch 325.00<br>OSF375-156 | **Patch:** Corrects ncheck -s Option Usage Problem<br>**State:** New<br>Corrects an AdvFS problem when running the ncheck utility with the -s option on an AdvFS file system, the command never returns but instead justs keeps using cpu cycles. This problem only occurs when there are no special files in the file system. |
| Patch 327.00<br>OSF375-158 | **Patch:** File Lock Corr(s), Filesystem Can Not Be Unmounted<br>**State:** Supersedes patches OSF375-350454 (282.00), OSF375-148 (317.00)<br>This patch corrects the following:<br>• Fixes a kernel memory fault panic in purge_fs_locks. This problem is normally only seen on ASE or TruCluster systems.<br>• Fixes several problems with vfs file locking that could cause a crash including the file lock adjust logic, delete sleep lock logic, dead file lock logic, check/change granted logic, and insert file lock logic.<br>• A filesystem cannot be unmounted and the system displays a "Device busy" error message. |
| Patch 329.00<br>OSF375-160 | **Patch:** 4GB Buffer R/W problem, poll() System Call As Timer<br>**State:** Supersedes patch OSF375-350397 (222.00)<br>This patch corrects the following:<br>• Fixes a read/write problem for buffers larger than 4GB. The read/write request would truncate to a maximum of 4GB, but return success, causing data corruption.<br>• Adds a mechanism to the poll() system call to allow it to be used as a timer. |
| Patch 332.00<br>OSF375-163 | **Patch:** Prevents "kernel memory fault" During Sync Operation<br>**State:** New<br>Prevents a "kernel memory fault" in the bread() routine while performing sync operations. |
| Patch 336.00<br>OSF375-168 | **Patch:** Include New Error Reporting Command, filterlog<br>**State:** New<br>This patch provides a new command, filterlog, which improves error reporting on AlphaServer 8200/8400 systems. |
| Patch 342.00<br>OSF375-175 | **Patch:** Corrects simple lock timeouts And kern mem Faults<br>**State:** New<br>Corrects a problem on DIGITAL's 8200/8400 machines where cpus may be bombarded with interrupts. The high amount of interrupts may cause simple lock timeouts and kernel memory faults. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 364.00<br>OSF375-174 | **Patch:** Host MIB and SNMP Correction<br>**State:** Supersedes patches OSF375-360066 (84.00), OSF375-360100 (229.00), OSF375-360114 (289.00), OSF375-360054 (82.00), OSF375-153 (322.00)<br>This patch corrects the following:<br>• Fixes the os_mibs source file, hrm_fs.c, which makes a call to the statfs function with 2 arguments, when statfs expects 3 arguments.<br>• Removes support for atTable, so that common applications (like NetView autodiscovery) will use the ipNetToMediaTable instead.<br>The SNMP agent returns incorrect data when requested for the MIB II Address Translation Table (atTable). The agent returns correct data for ipNetToMediaTable, which supersedes atTable in MIB II.<br>• Fixes memory leaks with the FDDI and Token Ring method routines used with Extensible SNMP subagent (ESNMP).<br>• The Host MIB code uses incorrect presentation names for some processors. This is seen when retrieving the MIB variable "hrDeviceDescr". This patch also adds presentation names for processors added in release v3.2g.<br>• Allows the extensible SNMP deamon to handle a very high volume of SNMP trap requests.<br>• Fixes the problem where a malformed trap message sent at boot-time by the DIGITAL UNIX SNMP daemon to a Windows NT Network Management Station (NMS) could cause the NMS application or the NT operating system to crash. |
| Patch 365.00<br>OSF375-176 | **Patch:** ed Command Correction<br>**State:** New<br>This patch fixes a problem in which the ed command when used with the -G option prints extra characters. |
| Patch 368.00<br>OSF375-180 | **Patch:** vdump & vrestore Command Corrections<br>**State:** New. Supersedes patches OSF375-350389 (240.00), OSF375-074 (215.00), OSF375-075 (216.00), OSF375-154 (323.00), OSF375-169 (337.00)<br>This patch corrects the following:<br>• Fixes a problem caused by the vrestore command. The command would fail when restoring multiple savesets from a TZS20 tape drive.<br>• Fixes a problem in which vrestore can cause an occasional core dump (Foating Exception).<br>• Fixes a problem in which the vrestore command is unable to read data from a raw disk partition.<br>• Fixes a problem where the vrestore program does not report failed exit status appropriately on incomplete or incorrect commands, corrupt or invalid saved sets, or file open failures.<br>• Fixes a problem in which the vrestore command fails when running multiple iterations of the command in a script or from the command line.<br>• Fixes a problem with the vrestore command. The command had returned a success status code even though it had restored an incomplete file during the operation. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 370.00<br>OSF375-184 | **Patch:** OSF375-184<br>**State:** New<br>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. DIGITAL has corrected this potential vulnerability. |
| Patch 371.00<br>OSF375-186 | **Patch:** lpq Print Subsystem Corrections<br>**State:** Supersedes patch OSF375-350392 (221.00)<br>This patch corrects the following:<br>• Fixes a problem where the lpq command causes the program to crash (segmentation fault).<br>• Improves the reliability and efficiency of DIGITAL UNIX print services. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 372.00<br>OSF375-187 | **Patch:** libc And Utility Corrections<br>**State:** Supersedes patches OSF375-350217 (93.00), OSF375-350222 (95.00) OSF375-350236 (101.00), OSF375-350253 (114.00), OSF375-350279 (126.00), OSF375-360053 (81.00), OSF375-360082 (180.00), OSF375-360082-1 (244.00), OSF375-350412 (268.00), OSF375-350449 (280.00), OSF375-002 (2.00), OSF375-085 (239.00), OSF375-360064 (83.00), OSF375-101 (251.00), OSF375-110 (259.00), OSF375-111 (260.00), OSF375-152 (321.00), OSF375-236 (415.00)<br>This patch corrects the following:<br>• Fixes a problem with the statvfs function. statvfs returns an incorrect status when the file system is full.<br>• Fixes a problem in which the vquota, vedquota, quota, edquota, dump, csh, and nslookup commands will sometimes display incorrect error messages for non-English locales.<br>• Fixes a problem in which RPC client functions do not correctly handle system calls interrupted by a signal (EINTR errors).<br>• Fixes a problem with the auditd daemon. If auditd is logging to a server and the server becomes unavailable, the CPU usage for the daemon rises dramatically.<br>• This patch allows system managers to both set and obtain quotas for users and groups which are numeric when using the edquota, vedquota, quota and vquota programs.<br>• Fixes a problem in which the 'date' command is unable to set the date to January 1, 1970 00:00:00 GMT or February 29, 2000.<br>• Enhancements to the date command for Year 2000 support.<br>• Fixes a problem where printing of a string with a specified precision could result in a segmentation fault.<br>• Fixes a TCP/IP problem that can occur with programs linked with the libc library. These programs may return a value of (-1) when calling the svc_tcp() function.<br>• A potential security vulnerability has been discovered in bind, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.<br>• /sbin/shutdown takes too long if there are many open LAT lines.<br>• This patch fixes a problem that occurs after a user logs into a system with an SRV4-style LAT device. When the ttyslot function is called, the system fails to find the device and returns a value of zero, indicating an error in the ttyslot function.<br>• The patch ensures that setlocale() does not call free() with a null pointer, which may crash an application that uses a third-party malloc package.<br>• sendmail would generate a core dump with a segmentation fault.<br>• problem in the filename pattern-matching behavior of the find command when it includes the "?" metacharacter. The bug actually resides in fnmatch(), which is used by find.<br>• A memory leak problem associated with the strxfrm() and wcsxfrm() functions and some incorrect behavior in __do_replacement(), which is used by both strxfrm() and strcoll().<br>• Fixes a problem with the edquota utility, which prevented a user from creating quotas for UIDs or GIDs that did not already exist in the /etc/passwd or /etc/group files.<br>This patch adds automatic detection of a cdfs file system for the mount(8) command. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 374.00<br>OSF375-189 | **Patch:** ksh Shell Correction<br>**State:** Supersedes patch OSF375-350239 (104.00)<br>This patch fixes the following problems:<br>• When editor options are set in ksh, ksh would not reset modes when ksh exited via a trap.<br>• Fixes a problem that was caused by the Korn shell running in EMACS mode. When a window was resized with a width that exceeded 160 characters, the next command (or even a return) would cause the ksh utility to core dump. |
| Patch 375.00<br>OSF375-190 | **Patch:** Tape Servicea Relocation Correction<br>**State:** New<br>This patch fixes a problem in which a a cluster member panics, when the Production Server or Available Server software attempts to relocate a tape service. |
| Patch 376.00<br>OSF375-191 | **Patch:** machine check Correction<br>**State:** New<br>This patch fixes the following problems that occur on AlphaServer 1000A 4/233 and 4/266 systems:<br>• If a machine check occurs, the register data written to the binary.errlog will show zeroes in all registers when viewed with DECevent.<br>• If a correctable memory error occurs, the system panics with a kernel memory fault. |
| Patch 378.00<br>OSF375-195 | **Patch:** Correction to Potential Problem to C-library Call<br>**State:** New<br>This patch corrects a potential problem in the handling of a ieee_get_state_at_signal(3) C-library call. |
| Patch 379.00<br>OSF375-196 | **Patch:** kloadsrv Will not be haulted in Single-User Mode<br>**State:** New<br>This patch ensures that kloadsrv remains running when the system is shut down to the single user run level. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 380.00<br>OSF375-197 | **Patch:** AdvFS Corrections<br>**State:** Supersedes patches OSF375-047 (47.00), OSF375-360041 (77.00), OSF375-360051 (80.00), OSF375-052 (52.00), OSF375-360067 (85.00), OSF375-360071 (87.00), OSF375-350324 (153.00), OSF375-360088 (197.00), OSF375-360090 (198.00), OSF375-077 (217.00), OSF375-360112 (288.00), OSF375-137 (172.00), OSF375-115 (264.00), OSF375-122 (294.00), OSF375-127 (299.00), OSF375-144 (314.00), OSF375-155 (324.00), OSF375-162 (331.00), OSF375-164 (333.00) OSF375-171 (361.00), OSF375-172 (362.00), OSF375-173 (363.00), OSF375-183 (369.00), OSF375-231 (411.00), OSF375-244 (421.00), OSF375-188 (373.00)<br>This patch corrects the following:<br>• Corrects a problem where the mcellCount on-disk was not being updated as files were being migrated and this resulted in a panic situation.<br>• Fixes AdvFS performance problems.<br>• Fixes an AdvFS problem that causes a lockmode 4 system panic.<br>• Corrects a situation where a quotacheck can cause a system panic.<br>• Fixes a kernel memory fault problem that occurs on AdvFS file systems. The system displays the following error message:<br>panic: kernel memory fault at spec_reclaim()<br>• Fixes a problem that occurs on AdvFS file systems where, under certain circumstances, modifications to mmaped data are not written to disk. This may result in data corruption.<br>• Corrects a problem with domain panics that could possibly cause the system to panic. A new AdvFS error number (E_DOMAIN_PANIC) (-1028) was created.<br>• Fixes a system panic when shutting down to single user mode using either one of the following commands when AdvFS is the root or usr filesystem:<br># shutdown now<br># init s<br>• Fixes a system panic with the following error message:<br>panic (cpu 0): kernel memory fault<br>• Fixes a problem with an NFS V3 mounted AdvFS file system where under heavy I/O load, data written to a file may be lost. Additionally, because file stats are not being saved, the file modification time may revert to a previous value.<br>• Fixes system panic with the following error message:<br>AdvFS exception Module=26 line=1483<br>• Fixes to prevent the following two panics:<br>AdvFS Exception Module = 1, line = 1891<br>and<br>kernel memory fault |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 380.00 continued | • This patch fixes a problem that occurs with the telnet and ftp commands. Telnet or ftp processes that are no longer in use, are left on the system indefinitely. When a user tries to log in, the login process hangs after displaying the last login message.<br>• Idle time is reset on broadcast message when AdvFS is the root file system.<br>• System panics with "kernel memory fault" in ubc_page_alloc().<br>• A problem in which a system using AdvFS can run out of metadata space when the AdvFS domain still has some free space available. The system will display error messages such as 'no space left on device'.<br>The problem may occur on a heavily fragmented system with many small files, such as an Internet News server or Mail server.<br>• A panic that is seen when running the auditd and auditing msfs_syscall. There will most likely be a lot of memory contention as well for this panic to be triggered.<br>• A problem in which the getrusage system call returns zero for the values of ru_inblock and ru_outblock on an AdvFS file system.<br>• Fixes NFS rpc.lockd "can't clear lock after crash of client" when AdvFS is being used.<br>• Prevents a "kernel memory fault" in the msfs_reclaim() routine on systems using AdvFS.<br>• Fixes a problem with the chfsets command. When a root user exceeded the fileset quota (which root is allowed to do), the chfsets command reported negative values for the free and available blocks in the fileset.<br>• Fixes a problem that occurs on AdvFS systems. The system will panic with the following error message:<br>malloc_overflow: guard space corruption<br>• Fixes a problem with the AdvFS fs_write routine, which would mishandle partial writes after detecting an error.<br>• Fixes a problem in AdvFS locking code which causes the following panic:<br>kernel memory fault<br>• Fixes a problem in AdvFS. AdvFS does not return an error when a user opens a file in O_SYNC mode and power is lost on the disk drive.<br>• Corrects a problem where a panic would occur when running rmtrashcan on a clone.<br>• Fixes a problem with AdvFS, which caused a system panic with the following message:<br>log_flush_sync: pingpg error<br>The system panic occurred when the AdvFS domain had already issued a domain panic and a user application then attempted to close a file in that domain. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 381.00<br>OSF375-199 | **Patch:** : Security, crontab (SSRT0487U)<br>**State:** Supersedes patches OSF375-350233 (99.00) OSF375-350291 (133.00), OSF375-167 (335.00), OSF375-105 (254.00)<br>This patch corrects the following:<br>• The following "at -t" command problems:<br>– The command did not work with user id's that were not in the password file.<br>– The command did not work on the leap year of 2000.<br>• Corrects several problems with the "at", "cron", and "crontab" commands.<br>• 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. DIGITAL has corrected this potential vulnerability. |
| Patch 383.00<br>OSF375-201 | **Patch:** High Activity Message Queue Hang Correction<br>**State:** New<br>This patch fixes a problem that occurs with applications based on POSIX message queues. During certain high activity periods, processes may hang when trying to access the message queue. |
| Patch 384.00<br>OSF375-202 | **Patch:** File Management, Security (SSRT0537U)<br>**State:** New<br>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. DIGITAL has corrected this potential vulnerability. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 386.00<br>OSF375-204 | **Patch:** Various Device Driver Corrections<br>**State:** Supersedes patches OSF375-370034 (65.00), OSF375-370043 (68.00), OSF375-068 (191.00), OSF375-365052 (192.00), OSF375-350309 (145.00), OSF375-073 (214.00), OSF375-365036 (71.00), OSF375-089 (246.00), OSF375-365068 (285.00), OSF375-095 (248.00), OSF375-112 (261.00), OSF375-141 (311.00), OSF375-161 (330.00)<br>This patch corrects the following:<br>• Fixes a problem that occurs when KZPSA and KZTSA hardware resources needed to do I/O are unavailable causing a large number of events to be logged. The system can become sluggish and sometimes crash. This problem is seen on 8400 and 4100 systems with limited hardware scatter-gather memory resources.<br>• Provides a set of workarounds for Qlogic firmware bugs. These bugs were encountered when using the HSZ70 Raid Array Controller on the KZPBA-CB wide differential UltraSCSI adapter in a dual-node cluster environment.<br>• Fixes a problem that occurs on AlphaServer 4100 systems. If no devices are attached to the KZPSA disk controller, the system may panic when attempting to perform I/O.<br>• After a disk error occurs, mirror set switching may not happen soon enough to ensure high availability, or in some cases may not happen at all.<br>• Provides the following support to DIGITAL UNIX V3.2G:<br>– Support the HSZ70 Raid controller on the Fast10 Wide Differential KZPSA adapter in cluster environments under V3.2G. Support of the HSZ70 Raid controller also requires the KZPSA firmware to be upgraded to at least the version distributed on the Version 5.0 AlphaServer Console Firmware CDrom.<br>– Performance regression fix for Qlogic isp1020/isp1040 chips.<br>– Provide SCSI target mode fixes for ASE/TCR support on QLogic, primarily for HSZ70 support.<br>– All modifications included in this patch are compatible with existing versions of KZPSA and Qlogic firmware.<br>• Adds device recognition for TZ89, TZS20, TZS2, TLZ10, and TLZ1 tape drives.<br>sim_err_sm Target went to command phase<br>sim94_intr Illegal command<br>panic: "xpt_callback: callback on freed CCB"<br>• Provides support for TZ89, and latent support for TZS20, TZS2, TLZ10, TLZ1.<br>• When HSZ50 hardware is installed, the system exhibits very slow performance.<br>• Provides the following additional event logging by the SCSI/CAM disk driver: Additional Unit Attention messages, additional details for hard errors logged after unsuccessful I/O recovery attempts, and provides informational messages on the progress of recovery events. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 386.00 continued | • Fixes various system problems:<br>– System panic with: "xpt_callback: callback on freed CCB".<br>– System panic with kernel memory fault while trying to remove an spo resource queue entry.<br>– Logging following group of 3 errors every few minutes: spo_verify_adap_sanity, spo_misc_errors, spo_bus_reset when the system was under heavy load.<br>– A tape drive was powered off for maintenance and disconnected, the HSZ40 was rebooted and the system then panicked with "simple_lock: time limit exceeded".<br>– Infrequently, under heavy disk I/O loads, user data can be written to the wrong disk, resulting in data corruption.<br>• Probe of isp fails intermittently during boot.<br>• A number of problems have been fixed in the ISP driver. These include: "minimum spl violation" panics with lockmode=4, simple lock time limit restart Qlogic(LUN queue after abort)" panics.<br>• Fixes a problem in which a failed KZPSA adapter panics the kernel. It also fixes a problem in which CAM status was returning an incorrect "NO HBA" status for miscellaneous SIMPORT errors, instead of the correct "CAM BUSY" status. |
| Patch 387.00<br>OSF375-205 | **Patch:** write lock Correction<br>**State:** New. Supersedes patch OSF375-178 (367.00)<br>This patch fixes the following problems:<br>• Fixes a problem that crashed the system while it was running a "collision" test. The process would hang on a lock, never be woken, and crash the system.<br>• Fixes a problem in AdvFS that produced the following system panic:<br>bs_logflush_start: cannot write lsn |
| Patch 389.00<br>OSF375-208 | **Patch:** AdvFS message Correction<br>**State:** New<br>This patch fixes a problem with messages in system logs that reported AdvFS user and group quota limits. The messages were unclear: the user could not determine from them which users or groups were reaching the quota limits. |
| Patch 390.00<br>OSF375-209 | **Patch:** System Crashes<br>**State:** New<br>This patch fixes a problem where the machine server system calls are not being type checked properly potentially causing system crashes by unprivileged programs. |
| Patch 391.00<br>OSF375-210 | **Patch:** Correction to kloadsrv(8)<br>**State:** New<br>This patch corrects a problem that would randomly cause kloadsrv(8) to crash and improperly load/unload modules. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 397.00<br>OSF375-216 | **Patch:** Corrects Several rpc.lockd Problems<br>**State:** Supersedes patch OSF375-350352 (181.00)<br>This patch corrects the following:<br>• NFS mounted file systems may hang.<br>• The rpc.lockd program may fail because it loses a message granting NLM approval.<br>• An NFS mounted file system may hang.<br>• The rpc.lockd daemon may crash with a core dump.<br>• An error occurs with NFS mounted user mail files. This error prevents the files from being locked and prints out the following message:<br>cannot lockf<br>• An NFS problem may occur and the system displays the following error message:<br>NFS error 48 cannot bind sockets<br>• Corrects two problems, the first change moves locked files from the message queue to the held list once. The second change adds code to allow locked files leftover from a server reboot, to timeout and be transmitted to the server. |
| Patch 398.00<br>OSF375-217 | **Patch:** overflow exception Correction<br>**State:** New<br>This patch fixes a problem that was caused by both floating point and integer overflow exceptions setting the si_code member in the siginfo structure to FPE_FLTOVF. |
| Patch 400.00<br>OSF375-219 | **Patch:** Automount Correction<br>**State:** New<br>This patch fixes an automount problem. An automount map file entry that included a comment was being parsed incorrectly, resulting in an error. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 401.00<br>OSF375-220 | **Patch:** Various NFS Filesystem Handling Correction<br>**State:** Supersedes patches OSF375-365034 (70.00), OSF375-365053 (202.00), OSF375-365053-1 (202.01), OSF375-365063 (234.00), OSF375-157 (326.00), OSF375-179 (346.00)<br>This patch corrects the following:<br>• 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. DIGITAL has corrected this potential vulnerability.<br>• Fixes a problem where the umount of a filesystem will fail with "mount device busy", but no processes are accessing files in the filesystem.<br>• Fix greatly reduces the number of "NFS stale file handle" messages logged to an NFS server system console.<br>• Allows some third-party NFS v2 clients to experience a performance improvement.<br>• This patch fixes a problem in which nfsportmon does not allow the root directory to be mounted from either a Solaris system or from an ULTRIX Version 4.2A system.<br>• Fixes a problem with NFS conversion of a file's vnode number to a file handle number. The file id was truncated improperly, generating EOVERFLOW errors. |
| Patch 402.00<br>OSF375-221 | **Patch:** showfile Command Correction<br>**State:** New<br>This patch fixes a problem with the showfile command, which incorrectly returned an error status when it attempted to display a file that was a symbolic link. |
| Patch 404.00<br>OSF375-223 | **Patch:** bufpages and bufcache corrections<br>**State:** New. Supersedes patch OSF375-213 (394.00)<br>This patch fixes the following problems:<br>• Fixes the bufpages calculation so that it takes granularity hints into account.<br>• Corrects a potential boot panic problem by limiting the size of the bufcache. |
| Patch 405.00<br>OSF375-224 | **Patch:** cron Command Problem Correction<br>**State:** Supersedes patch OSF375-350390 (241.00)<br>This patch fixes the following problems:<br>• Fixes a problem in which the cron command deletes non-local file system files mounted in either the /tmp, /var/tmp, or /var/preserve directories.<br>• Prevents the crontab file from incorrectly deleting files found in file systems mounted under the /var/preserve, /tmp, and /var/tmp directories. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 406.00<br>OSF375-226 | **Patch:** syslogd Cannot Write /dev/console, (SSRT0499U)<br>**State:** Supersedes patches OSF375-350188 (245.00), OSF375-350383 (219.00), OSF375-099 (170.00), OSF375-128 (300.00), OSF375-143 (313.00), OSF375-222 (403.00)<br>This patch corrects the following:<br>• Fixes a problem in which the syslogd daemon may hang when writing to a named pipe log file.<br>• Fixes a panic that occurs when the system's message buffer size is increased to beyond the default size of 4096. During the subsequent reboot, the syslogd daemon fails with a "Segmentation fault (core dumped)" message, and creates a core file in the "/" directory.<br>• 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.<br>• Fixes a problem where the syslogd program cannot properly forward large messages to remote systems. It will either write them to the wrong facility (specified in /etc/syslog.conf) or write incomplete data.<br>• After a login session on /dev/console exits, syslogd cannot write to /dev/console.<br>• Fixes a problem in which savecore incorrectly reports a negative number of dumped bytes. This problem may be seen when doing a full crash dump on a system that has more then 2 gigabytes of memory.<br>• Fixes a problem in which syslogd will core dump if /etc/syslog.auth file has greater than 23 lines. |
| Patch 407.00<br>OSF375-227 | **Patch:** Mail Corrections, Security (SSRT0421U)<br>**State:** Supersedes patches OSF375-350254 (115.00), OSF375-350331 (154.01)<br>This patch corrects several mail problems.<br>• This patch fixes two problems with the mail utility:<br>– Mail cannot be sent to usernames consisting of uppercase and lowercase letters.<br>– Mail fails when a large distribution list is used.<br>• Fixes a problem with the sendmail program. Sendmail would dump core and not process any more jobs in the queue when it encountered control characters in a qf file. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 408.00<br>OSF375-228 | **Patch:** Mem Handling And File System Operation Corr(s)<br>**State:** Supersedes patches OSF375-360037 (75.00), OSF375-360050 (79.00), OSF375-049 (49.00), OSF375-050 (50.00), OSF375-056 (56.00), OSF375-350435 (275.00), OSF375-096 (249.00), OSF375-125 (297.00), OSF375-130 (301.00), OSF375-149 (318.00), OSF375-165 (334.00), OSF375-177 (366.00), OSF375-214 (395.00)<br>This patch corrects the following:<br>• Fixes a panic in the virtual memory management system. The system displays the following error message:<br>trap: invalid memory read access from kernel mode<br>• Fixes the panic "vm_object_free: res count > 1".<br>• Corrects a problem in which a filesystem may fail to unmount during shutdown or reboot. An error message similar to the following is displayed:<br>msfs_unmount EBUSY failed for usr with error 16 during shutdown<br>• Fixes an NFS problem that causes the system to hang.<br>• Fixes a file corruption problem that may occur with certain applications, for example Realtime applications, that use the plock() system call or the mlock() and mlockall() library routines.<br>• Fixes a problem that causes systems to panic with a "kernel memory fault" from u_dev_lockop(). This has happened when a database tried to memory map a file.<br>• This patch fixes a problem in which processes can hang waiting for a system call to table() to complete.<br>• A problem in which the system will panic with:<br>"u_shm_oop_deallocate: reference count mismatch"<br>• A problem in which the system will panic:<br>"pmap_remove_range: page wired"<br>• A PATHWORKS client does not see all the files in a directory when the directory is an NFS mounted OpenVMS UCX exported directory.<br>• Fixes a problem in which mmap activity to a file that is NFS mounted may cause the client process to hang after the file is deleted.<br>• Fixes a problem that produced a deadlock betweeen process threads. Typically, the deadlock caused the msfs_getpage routine to wait forever for a lock to be released.<br>• Prevents a kernel malloc leak when changing the protection of a System V shared memory region that uses gh-chunks.<br>• Fixes a virtual memory problem in which an uninitialized pointer in u_dev_protect() causes a kernel memory fault to occur. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 409.00<br>OSF375-229 | **Patch:** Corrections to AdvFS message, linking<br>**State:** New. Supersedes patch OSF375-200 (382.00)<br>This patch fixes the following problems:<br>• Fixes a problem with an unclear AdvFS message. When trying to mount an AdvFS fileset on a system that did not have AdvFS installed, the following message was displayed:<br>No such device<br>Now, in similar cases, the following AdvFS message is displayed:<br>Cannot mount AdvFS fileset, AdvFS not installed<br>• Fixes a problem with AdvFS and links in the /etc/fdmns directory. Previously, AdvFS did not ensure that every link in a directory entry pointed to a block device. Now, it does. |
| Patch 410.00<br>OSF375-230 | **Patch:** Correction to a Compiler Problem<br>**State:** New<br>This patch fixes a compiler problem that was causing CPU EXCEPTION errors to be generated in the system binary error log. The problem was experienced during bootstrap on 2100A cpus. |
| Patch 412.00<br>OSF375-232 | **Patch:** Corrects Return Error Status For POSIX Compliance<br>**State:** New. Supersedes patch OSF375-147 (316.00)<br>This patch fixes the following problems:<br>• Corrects the return error status on reads and writes in LSM to make it POSIX compliant.<br>• Fixes a problem in lsm. A data corruption occurs when readv/writev coallesced via physio while in read/writeback mode. |
| Patch 413.00<br>OSF375-233 | **Patch:** Correction to User Stack Pointer Handling<br>**State:** New<br>This patch fixes a problem with user stack pointers not being saved properly in kernel crash dumps for running threads. |
| Patch 414.00<br>OSF375-234 | **Patch:** dd Command Corrections<br>**State:** Supersedes patches OSF375-350359 (184.00), OSF375-132 (303.00)<br>This patch corrects the following:<br>• Fixes a problem when the seek option to the dd command is used to insert data into an existing output file, the resulting file is incorrect and all of the original data is lost.<br>• Fixes a problem in which the dd command can corrupt output on very large files (2 GB or greater) when the "conv=sparse" option is used.<br>• Fixes a problem with the dd command in which dd aborts after a read error. This problem occurs even when the "conv=noerror" parameter is specified. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 417.00<br>OSF375-238 | **Patch:** Various Kernel Corrections<br>**State:** Supersedes patches OSF375-055 (55.00), OSF375-360070 (86.00), OSF375-360070-1 (86.01), OSF375-360070-2 (86.02), OSF375-360076 (89.00), OSF375-360076-1 (89.01), OSF375-360085 (187.00), OSF375-365050 (243.00), OSF375-360087 (196.00), OSF375-370048 (207.00), OSF375-350372 (204.00), OSF375-069 (206.00), OSF375-360101 (230.00), OSF375-350438 (242.00), OSF375-365070 (286.00), OSF375-365071 (287.00), OSF375-350448 (279.00), OSF375-119 (283.00), OSF375-120 (292.00), OSF375-135 (306.00), OSF375-150 (319.00), OSF375-151 (320.00), OSF375-211 (392.00), OSF375-215 (396.00)<br>This patch corrects the following:<br>• Fixes problems with missing/lost signals that can cause applications to hang. In particular, the DECss7 product may experience severe problems. The problem happens primarily with POSIX signals.<br>• Corrects a kernel memory fault panic in routine pmap_pt_access().<br>• Fixes a "simple lock time limit exceeded" panic from the procfs subsystem.<br>• Fixes a kernel memory fault in the u_anon subsystem.<br>• Fixes a system crash when setting the date on SMP systems.<br>• Fixes fixes a problem that occurs when starting up a system that is running the auditing subsystem and the performance manager. The system panics with the error message:<br>kernel memory fault<br>• Fixes a problem that may occur after a system panics. The system may hang when trying to do a crash dump.<br>• Fixes an I/O queue corruption problem that occurs during normal shut down of SMP systems with AdvFS.<br>• Fixes a problem in which panics will occur if an attempt is made to run a shell script residing on any filesystem mounted with the "noexec" option.<br>• Fixes the corruption of core files produced by applications with 15 or more threads.<br>• Fixes three system panics; no special situation that will cause these panics:<br>– Fixes a panic that prints "kernel memory fault".<br>– Fixes a panic that prints "pmap_dup: level3 PTE not valid".<br>– Fixes a panic that prints "delete_pv_entry: mapping not in pv_list".<br>• Fixes a problem with the exec() system function where a shell script that has "#! " as the first line of the script, invokes the program but does not set the effective user id for the execution of the program.<br>• Fixes a problem that occurs on AlphaServer 8200 and 8400 systems when a processor fails to restart after a user halts the system by entering "Control-P Control-P" and then typing "continue" on the console. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 417.00 continued | • Fixes problem when debugging multithreaded applications with Ladebug, debugging sessions may hang due to a bug in procfs (e.g., /proc filesystem).<br>• Fixes system crash when setting the date for SMP systems.<br>• This patch fixes a problem in which the the lastcomm accounting command doesn't print the "S" flag at appropriate times. This patch also improves the performance of lastcomm.<br>• This patch enables the latest Informix KAIO functionality. The patch should be installed by Informix customers using the Informix 7.20.UC4 release. The Informix defect number 40041 regarding KAIO is fully addressed by this patch. The patch is required when this message appears, followed by a core dump with the SIGABRT signal:<br>Internal AIO consistency error:<br>No fork for group completion. Aborting.<br>• Fixes a number of problems relating to signals and POSIX 1003.1b timers in multithreaded programs running on multiprocessor systems. These problems can result in missed timer-expiration signals and system crashes.<br>• This patch fixes some hangs that can occur during the "syncing disks..." portion of panic processing, improves the reliability of getting a dump after a system panic, and also makes it more likely that AdvFS buffers will be synced to disk after a system panic.<br>• Removes extraneous debug code.<br>• Fixes a problem that can cause asynchronous I/O to fail.<br>• Fixes a problem with the way the ps utility collected CPU usage information. One effect of the problem was that processes run with nice values of 18 or greater had contention problems based on the incorrect CPU values. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 418.00<br>OSF375-240 | **Patch:** Corr(s) for Kernel, Network, Security (SSRT0476U)<br>**State:** Supersedes patches OSF375-370033 (64.00), OSF375-370044 (69.00), OSF375-350252 (113.00), OSF375-350316 (149.00), OSF375-350411 (228.00), OSF375-350422 (273.00), OSF375-350440 (276.00), OSF375-053 (53.00), OSF375-062 (62.00), OSF375-082 (236.00), OSF375-113 (262.00), OSF375-134 (305.00), OSF375-146 (315.00), OSF375-159 (328.00)<br>This patch corrects the following:<br>• Fixes a problem that occurs on an SMP system when running STREAMS. The system panics with the following error message:<br>"kernel memory fault"<br>Also the ASDU netbeui server (nbelink) will not close a connection. It will hang in dlcb_close awaiting a STREAMS event. Subsequently, new connections will not be able to connect to nbelink.<br>• Fixes a problem in the streams code which could have resulted in data corruption.<br>• Fixes a problem when printing to slow printers using DIGITAL UNIX LAT. The end of a large file fails to print and no error is reported.<br>• A potential security vulnerability has been discovered, where under certain circumstances, a kernel memory fault panic may occur.<br>• Fixes a problem that occurs when running STREAMS. The system panics with a kernel memory fault in either osr_run() or osr_reopen().<br>• This patch fixes a problem that causes the system to panic with a kernal memory fault or "malloc_audit: guard space corruption" with osr_run as an entry in the stack.<br>• This patch fixes a kernel memory fault panic. This panic occurs on systems running System V applications or any user process compiled with the System V environment, even if System V is not loaded on the system.<br>• Fixes the problem of a system hang due to corruption of a STREAM synchronization queue's forward pointer. The system hangs in the csq_cleanup() function.<br>• Fixes the problem where applications running System V pseudoterminal slave pty can hang forever on open() system call.<br>• Fixes a wide variety of system panics and other problems caused by random memory corruption. Problem noticed at sites hosting a lot of streams activity.<br>• Allows a customer-written device driver to return the customer's own local error value. Without this patch, the user process will get EINVAL instead.<br>• Fixes a problem that causes the system to "assert_wait" panic with streams code on the stack.<br>• Fixes a situation in which the SVR4 STREAMS documentation could be violated. It allows a device number to be pushed on the stream.<br>• Replace Manual Installation Edit Instructions for OSF375-370033 in setld patch kit. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 418.00 continued | • This patch is an upgrade/replacement for the FAA FDDI driver and fixes a halt/restart problem found in the old driver. The old driver could panic a system with a "simple_lock_fault violation" during a re-initialization.<br>• Fixes a problem in which the system may panic with the following error message "kernel memory fault". |
| Patch 419.00<br>OSF375-241 | **Patch:** cam_tape Panics Correction<br>**State:** Supersedes patches OSF375-360052 (194.00), OSF375-360078 (90.00), OSF375-206 (388.00), OSF375-218 (399.00)<br>This patch corrects the following:<br>• Fixes a "simple_lock: time limit exceeded" panic.<br>• Fixes a "simple_lock: time limit exceeded" panic originating from either:<br>– ctape_close() routine<br>– ctape_strategy() routine<br>• Fixes a problem where during tape operations, the SPACE commands can not be interrupted.<br>• Fixes an ASE NFS problem that occurs on ASE systems with KZPBA disk controllers. The system crashes with a "simple_lock timeout" panic.<br>• Under certain conditions, the message "ctape_strategy: READ case and density info not valid." was being printed for every read from tape. This change will print the message only once. |
| Patch 420.00<br>OSF375-243 | **Patch:** Routing Correction<br>**State:** New<br>This patch fixes a routing corruption that could been seen as a kernel memory fault or a corruption within the 128 byte kernel memory bucket. |
| Patch 422.00<br>OSF375-246 | **Patch:** sh and rsh Command Corrections<br>**State:** Supersedes patch OSF375-350256 (117.00)<br>This patch fixes the following problems:<br>• Fixes two problems that occur when an application is started from a subshell, for example, sh -c <command>.<br>– An application will hang if it receives an interrupt signal, for example, if the user enters Ctrl/C.<br>– While an application is running, if Ctrl/C is entered, the parent process exits, but the child process remains.<br>• Fixes a problem where the performance of the Bourne shell may be slow when there are many automounted directories in the search path (as defined by the PATH environment variable). |
| Patch 424.00<br>OSF375-350230A | **Patch:** uid/gid From cd_defs Library Function Correction<br>**State:** Supersedes patch OSF375-350230 (96.00)<br>This patch corrects a problem with the cd_defs() function of libcdrom where cd_defs(CD_GETDEFS) returns the wrong default gid and uid for an ISSO 9660 CD-ROM. |
| Patch 425.00<br>OSF375-350230B | **Patch:** Wrong Default uid/gid From cd_defs Library Function<br>**State:** Supersedes patch OSF375-350230 (96.00)<br>This patch corrects a problem with the cd_defs() function of libcdrom where cd_defs(CD_GETDEFS) returns the wrong default gid and uid for an ISSO 9660 CD-ROM. |

**Table 3–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 426.00<br>OSF375-350244A | **Patch:** LSM Configuration Database Corrections<br>**State:** Supersedes patches OSF375-350243 (107.00), OSF375-350244 (108.00)<br>This patch corrects the following:<br>• A problem in which an LSM configuration database becomes corrupted when it grows beyond 128 KB. The LSM daemon displays an error message similar to the following when it starts up:<br>bad magic number<br>• Several problems that occur during certain LSM operations involving disklabel changes. |
| Patch 427.00<br>OSF375-350244B | **Patch:** LSM Corrections<br>**State:** Supersedes patches OSF375-350243 (107.00), OSF375-350244 (108.00)<br>This patch corrects the following:<br>• A problem in which an LSM configuration database becomes corrupted when it grows beyond 128 KB. The LSM daemon displays an error message similar to the following when it starts up:<br>bad magic number<br>• Several problems that occur during certain LSM operations involving disklabel changes. |
| Patch 428.00<br>OSF375-350378A | **Patch:** libcurses tparm Correction<br>**State:** Supersedes patch OSF375-350378 (211.00)<br>Fixes a problem in which the tparm routine in the libcurses.a library does not support more than a three digit value for its input parameter. |
| Patch 429.00<br>OSF375-350378B | **Patch:** libcurses tparm Routine Correction<br>**State:** Supersedes patch OSF375-350378 (211.00)<br>Fixes a problem in which the tparm routine in the libcurses.a library does not support more than a three digit value for its input parameter. |
| | |
| | |

# 4

# Summary of TruCluster Software Patches

This chapter summarizes the TruCluster software patches included in Patch Kit-0005.

Table 4–1 lists patches that have been updated.

**Table 4–1: Updated TruCluster Software Patches**

| Patch IDs | Change Summary |
|---|---|
| Patch 22.00, 15.00 | New |
| Patch 17.00 | Superseded by Patch 22.00 |
| Patches 5.00, 16.00, 23.00 | Superseded by Patch 26.00 |
| Patches 6.00, 9.00 | Superseded by Patch 21.00 |
| Patches 12.00, 18.00, 19.00, 24.00, 25.00 | Superseded by Patch 27.00 |
| Patches 12.00, 18.00, 19.00, 24.00, 25.00 | Superseded by Patch 28.00 |
| Patch 14.00 | Superseded by Patch 20.01 |

Table 4–2 provides a summary of patches in Patch Kit-0005.

**Table 4–2: Summary of TruCluster Patches**

| Patch IDs | Abstract |
|---|---|
| Patch 1.00<br>TCR100-001 | **Patch:** Function Naming And Kernel Build Failure Correction<br>**State:** Existing<br>Backport changes to function names and data symbols. This fixes problems where some function names in TCR V1.0 collided with function names in X.25 V2.0 causing the kernel build to fail. |
| Patch 2.00<br>TCR100-002 | **Patch:** Support The DEVGETGEOM ioctl And SAP R3<br>**State:** Existing<br>This patch allows the DRD subsystem to support the DEVGETGEOM ioctl. This change is necessary for support of SAP R3 with TruCluster software. |
| Patch 7.00<br>TCR100-008 | **Patch:** Disk Label Re-Init, Retry Command Correction<br>**State:** Existing<br>This patch fixes the following problems with Logical Storage Manager (LSM) volumes in DECsafe Available Server (ASE) and TruCluster environments:<br>• After installing a patch to the LSM voldisk command, the disk labels of LSM disks are inadvertently being reinitialized during service modification. This causes attempts to start the service to fail and leaves the service unassigned.<br>• Certain LSM operations that should have been retried were failing on the first attempt.<br>• Retry messages were not being printed to the log file. |

**Table 4–2: Summary of TruCluster Patches (cont.)**

| | |
|---|---|
| Patch 8.00<br>TCR100-009 | **Patch:** Correction For Service Aliases<br>**State:** Existing<br>This patch fixes a problem in /var/opt/TCR100/ase/sbin/nfs_ifconfig that corrupts the memory resident routing table and subsequent netstat output (netstat -r) during ASE service failover. |
| Patch 10.00<br>TCR100-011 | **Patch:** Cluster transition Problem Corrections<br>**State:** Supersedes patch TCR100-003 (03.00), TCR100-005 (04.00)<br>This patch fixes the following problems:<br>• This patch is a software workaround for a hardware problem with CCMAA-AA MEMORY CHANNEL adapters that may cause a cluster to hang or panic during node transitions. (Clusters using only CCMAA-BA MEMORY CHANNEL adapters do not exhibit this problem.)<br>• Patch to fix process space remote sync page deallocation.<br>• Backporting fix to check for valid state (FAILOVER_DONE) during failover. Not checking for this condition was causing a hang. |
| Patch 11.00<br>TCR100-012 | **Patch:** Panic During A Shutdown Correction<br>**State:** Existing<br>This patch corrects a problem whereby the ASE agent daemon (aseagent), ASE director daemon (asedirector), the trigger-action server daemon (tractd), or the submon process fails and exits without a core file if a SIGPIPE or other stray signal occurs. |
| Patch 13.00<br>TCR100-014 | **Patch:** Recognize KZPBA Correction<br>**State:** Existing<br>This patch adds KZPBA controller support for the ase_fix_config utility. |
| Patch 15.00<br>TCR100-016 | **Patch:** Workaround To vquotacheck Command Panic Correction<br>**State:** New<br>Fixes a problem in which running the vquotacheck command on a filesystem participating in an ASE service will cause a system to panic if the service fails over or relocates while the command is in progress. |
| Patch 20.01<br>TCR100-021-1 | **Patch:** System Panic, SCSI Error Condition Correction<br>**State:**New. Supersedes patch TCR100-015 (14.00)<br>This patch fixes the following problems:<br>• Fixes the following problems in the ASE Availability Manager (AM):<br>– A "simple_lock: time limit exceeded" panic on multi-processor, and system hangs in single processor systems. This can occur when multiple host target mode requests are issued due to SCSI aborts and resets on a shared bus.<br>– A kernel memory fault panic caused by a race condition when the AM de-initializes.<br>• This patch is part of the set of DIGITAL UNIX patches required to support the HSZ70 UltraSCSI Raid Array controller on the KZPSA adapter under TCR 1.0. |

**Table 4–2: Summary of TruCluster Patches (cont.)**

| | |
|---|---|
| Patch 21.00<br>TCR100-022 | **Patch:** Lock Trans ID, Group ID And Lock Processing Corr<br>**State:** Supersedes patches TCR100-007 (6.00), TCR100-010 (9.00)<br>This patch fixes the following problems:<br>• Fixes two problems in the TruCluster Distributed Lock Manager (DLM):<br>– A process's effective group ID not being checked when a process attempts to join a namespace. -<br>– Repeated calls to the dlm_quecvt function would erroneously return DLM_LKBUSY status.<br>• Corrects an assertion panic that occurs after a large number of transactions are made using the same lock. The assertion panic is triggered by integer wrapping of the lock transaction ID field. The system may panic with "dlm_panic". The actual assertion message is "<lkbp—>txid == 0>".<br>• Fixes a problem that can cause a cluster member to panic in rcv_deqlk_msg() with the panic string set to:<br>dlm_panic |
| Patch 22.00<br>TCR100-023 | **Patch:** Panic During Transition Correction<br>**State:** New. Supersedes patch TCR100-018 (17.00)<br>This patch fixes the following problems:<br>• Allows more time to remove a node from an 8-node cluster before causing the system to panic.<br>• Fixes a problem that can cause a "sysconfig -q rm" command to crash a cluster member. |
| Patch 26.00<br>TCR100-027 | **Patch:** ASE Data Base For LSM Correction<br>**State:** Supersedes patches TCR100-006 (5.00), TCR100-017 (16.00), TCR100-024 (23.00)<br>This patch fixes the following problems:<br>• Fixes a problem where changes in the LSM configuration were not being properly handled during the delete of an LSM volume from a service.<br>• Increases the timeout values for the LSM action scripts that are part of the TruCluster Production Server, Available Server and DECsafe Available Server products. The timeouts were too small for large LSM configurations and, under certain conditions, would cause the start of the services to fail, leaving them unassigned.<br>• Fixes a problem in ASE where removing a volume from an AdvFS domain mounted by an ASE service causes the service to fail to restart. The daemon.log says "I/O error".<br>• Fixes a problem in which under certain circumstances, an ASE service modification could result in a corrupted configuration data base. |

**Table 4–2: Summary of TruCluster Patches (cont.)**

| | |
|---|---|
| Patch 28.00<br>TCR100-026B | **Patch:** Not Properly Handling Error Condition Correction<br>**State:** Supersedes patches TCR100-013 (12.00), TCR100-019 (18.00), TCR100-020 (19.00), TCR100-025 (24.00), TCR100-026 (25.00)<br>This patch fixes the following problems:<br>• Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and Production Server software. When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied:<br>msgSvc: message queue overflow, LOST MESSAGE!<br>From this point on, no further messages will be received.<br>• Fixes a problem that may occur in an ASE (either DECsafe ASE Version 1.3, TruCluster Available Server, or TruCluster Production Server) when the ASE encounters connection attempts from hosts whose IP addresses cannot be resolved to hostnames. Instead of printing a warning about a possible security breach, the ASE daemons will core dump with a segmentation violation. One cause of this problem may be unknown hosts on the network using public domain internet security software which scans all TCP ports on remote hosts.<br>• Fixes a problem in TruCluster Production Server Software that can cause a cluster member to panic during a shutdown. One of the following panics will be issued by the distributed lock manager (DLM) if it attempts to rebuild the member's lock database and the connection manager daemons were already killed before they were able to stop all DLM activity:<br>rcv_credir_req: illegal state<br>rcv_crelk_req: illegal state<br>rcv_newlk_req: illegal state<br>• 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.<br>• Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. |

**Table 4–2: Summary of TruCluster Patches (cont.)**

| | |
|---|---|
| Patch 29.00<br>TCR100-031 | **Patch:** asemgr Core Dumps<br>**State:** Supersedes patches TCR100-013 (12.00), TCR100-019 (18.00), TCR100-020 (19.00), TCR100-025 (24.00), TCR100-026 (25.00), TCR100-026A (27.00)<br>This patch fixes the following problems:<br>• This patch corrects a problem in which the asemgr can core dump when adding a member back into an ASE.<br>• Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and Production Server software. When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied:<br>msgSvc: message queue overflow, LOST MESSAGE!<br>From this point on, no further messages will be received.<br>• Fixes a problem that may occur in an ASE (either DECsafe ASE Version 1.3, TruCluster Available Server, or TruCluster Production Server) when the ASE encounters connection attempts from hosts whose IP addresses cannot be resolved to hostnames. Instead of printing a warning about a possible security breach, the ASE daemons will core dump with a segmentation violation. One cause of this problem may be unknown hosts on the network using public domain internet security software which scans all TCP ports on remote hosts.<br>• Fixes a problem in TruCluster Production Server Software that can cause a cluster member to panic during a shutdown. One of the following panics will be issued by the distributed lock manager (DLM) if it attempts to rebuild the member's lock database and the connection manager daemons were already killed before they were able to stop all DLM activity:<br>rcv_credir_req: illegal state<br>rcv_crelk_req: illegal state<br>rcv_newlk_req: illegal state<br>• 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.<br>• Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. |