Tru64 UNIX and TruCluster Server Version 5.1B

Patch Summary and Release Notes for Patch Kit 1

December 2002

This manual contains information specific to Patch Kit 1 of the Tru64 UNIX operating system and TruCluster Server software products for Version 5.1B. It briefly describes the patches contained in this kit and provides information you should be aware of when installing certain patches.

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

Hewlett-Packard Company
Palo Alto, California

19–Dec-02

Contents

About This Manual

This manual contains information specific to Patch Kit 1 of the Tru64 UNIX operating system and TruCluster Server software products for Version 5.1B. It briefly describes the patches contained in this kit and provides information you should be aware of when installing certain patches.

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 Provides information about the Tru64 UNIX patches included in this kit.

Chapter 2 Provides information about the TruCluster Server software patches included in this kit.

Related Documentation

In addition to this manual, the following documentation may be helpful in the patching process:

- Tru64 UNIX and TruCluster Server *Patch Kit Installation Instructions*
- The `dupatch`(8) reference page, which describes the use of `dupatch` from the command line. This reference page is installed when you install the `dupatch` tools.
- Tru64 UNIX *Installation Guide*
- Tru64 UNIX *System Administration*
- TruCluster Server *Cluster Installation*
- TruCluster Server *Cluster Administration*
- Release-specific installation documentation

Patch Process Resources

We provide Web sites to help you with the patching process:

- To obtain the latest patch kit for your operating system and cluster:

  `http://ftp1.support.compaq.com/public/unix/`

- To view or print the latest version of the *Patch Kit Installation Instructions* or the *Patch Summary and Release Notes* for a specific patch kit:

  `http://www.tru64unix.compaq.com/docs/patch/`

- To visit our main support page:

  `http://www.compaq.com/support/index.shtml`

- To visit the Tru64 UNIX homepage:

  `http://www.tru64unix.compaq.com/`

Reader's Comments

We welcome any comments and suggestions you have on this and other Tru64 UNIX manuals.

You can send your comments in the following ways:

- Fax: 603-884-0120 Attn: UBPG Publications, ZK03-3/Y32
- Internet electronic mail:

  `readers_comment@zk3.dec.com`

  A Reader's Comment form is located on your system in the following location: `/usr/doc/readers_comment.txt`
- Mail:

  Hewlett-Packard Company
  UBPG Publications Manager
  ZK03-3/Y32
  110 Spit Brook Road
  Nashua, NH 03062-9987

Please include the following information along with your comments:

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

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

1

Tru64 UNIX Patches

This chapter provides information about the patches included in Patch Kit 1 for the base operating system. It also includes any general information about working with these patches.

This chapter is organized as follows:

- Section 1.1 provides release notes that are specific to the Tru64 UNIX patches in this kit, as well as release notes that are of general interest.
- Section 1.2 provides brief descriptions of the Tru64 UNIX patches included in this kit.

1.1 Release Notes

This section provides release notes that are specific to the Tru64 UNIX patches in this kit, as well as release notes that are of general interest.

1.1.1 Required Storage Space

Approximately 250 MB of temporary storage space is required to untar the base and TruCluster components of this patch kit. We recommend that this kit not be placed in the `/`, `/usr`, or `/var` file systems because doing so may unduly constrain the available storage space for the patching activity.

The following permanent storage space is required to install the base component of this patch kit:

- Approximately 47 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.
- Approximately 48 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.
- Approximately 593 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.
- Approximately 176 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

See Section 2.1.1 for information on space needed for the TruCluster Server patches.

1.1.2 Problem Seen on Systems with Smart Array Controller

This section describes the steps you should take if your system is configured with a Smart Array controller and you see the following event logged:

```
Host name: unx104
SCSI CAM ERROR PACKET
SCSI device class: CISS (Smart Array)
Bus Number: 6
Target Number: 4
Lon Number: 0
…
...
Event Information: Command timed out...resetting controller
```

If this occurs, take the following steps:

1. Create a file named `ciss.temp` with the following lines:

   ```
   ciss:
   ciss_throttle_threshold=5
   ```

2. Execute the following command:

   ```
   # sysconfigdb -m -f ciss.temp
   ```

3. Reboot your system:

   ```
   # shutdown -r now
   ```

1.1.3 Broken Links Reported During Baselining

When performing a baseline analysis with the `dupatch` utility, you will encounter the following message during Phase 4:

```
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:
      ----------------------------------------

  ./etc/lprsetup.dat                                          OSFPRINT540       UNKNOWN
  ./usr/share/doclib/annex/man/man3/Thread.3                  OSFTCLBASE540     UNKNOWN
      BROKEN HARDLINK TO ./usr/share/doclib/annex/man/man3/Tcl_ConditionNotify.3
  ./usr/share/doclib/annex/man/man3/Tcl_ConditionNotify.3     OSFTCLBASE540     UNKNOWN
      BROKEN HARDLINK TO ./usr/share/doclib/annex/man/man3/Thread.3

    Press RETURN to proceed...
```

You can disregard this information. The presence of these broken links will not affect your system operation, the installation of `dupatch` or `dupatch` tools, the successful installation of patches, or the rebuilding of kernels on the system.

1.1.4 New Russian Keyboard (Patch 339.00)

The new Russian 3R-LKQ48–BT keyboard, for which Patch 339.00 provides an updated keyboard map, comes with five extra keycaps. To enable any of those extra keycaps, you will need to modify the file `/usr/lib/X11/xkb/symbols/digital/russian`. For example:

```
//    KEY <AD09> can be replaced by an extra keycap.
//    If you replace it with the extra keycap, please uncomment
//    the following definition and comment out the original one.
//
//    key <AD09> {
//      symbols[Group1]=3D [               o,               O ],
//      symbols[Group2]=3D [     Ukrainian_i,     Ukrainian_I ]
//    };
    key <AD09> {
        symbols[Group1]=3D [               o,               O ],
        symbols[Group2]=3D [  Cyrillic_shcha,  Cyrillic_SHCHA ]
    };
```

1.1.5 Panics May Occur on Multi-CPU Systems

Boot-time panics may occur on multi-CPU systems if all of the following conditions exist:

- Auditing is enabled

- Audit's `-m` switch is configured to establish a dump interval
- The system contains empty CPU slots

The panic will occur on the first reboot after audit is configured or following an update installation on a system with audit already configured with a dump interval. The system will be unable to reboot in this configuration.

To work around this problem, boot to single-user mode and remove the `-m` option from the audit configuration stored in `/etc/rc.config.common` or `/etc/rc.config`.

The problem will be fixed in the next patch kit.

1.1.6 General and Problem Information for AlphaServer ES47, ES80, and GS1280 Systems

The following information pertains to the new AlphaServer ES47, ES80, and GS1280 systems, which require Tru64 UNIX Version 5.1B and this patch kit to be installed.

1.1.6.1 CPU Offline Restrictions

The Primary CPU cannot be taken off line.

CPUs that have I/O hoses attached to them can only be taken off line if another CPU without I/O attached is present in the system . A failure to adhere to this restriction will cause the `psradm` command to return an error.

In a two CPU configuration, the AlphaServer ES47 and ES80 do not allow any CPUs to be taken off line.

1.1.6.2 Problem with Capacity on Demand Process

A problem has been discovered with the capacity on demand process in which a CPU can be designated as spare, but is not taken off line as expected.

With the capacity on demand process, the `codconfig` *`[cpu_id_list]`* command lets you specify which CPUs you have paid for and which are spares. The command is supposed to mark the others as spare and then take them off line. Once a CPU is marked as spare, the `hwmgr` command and Manage CPUs SUITLET will not let you put them on line until you use the `ccod -l` or `ccod -p` command to either loan or purchase the CPU.

The workaround to the problem is to use the `codconfig` *`[cpu_id_list]`* command to mark the CPUs as spare and then use either the `hwmgr` command or the Manage CPUs SUITLET to take them off line (sometimes referred to as offlining them). In the following example, N is the CPU number.

```
# hwmgr -offline -name cpuN
```

If, for example, the `codconfig` command returns the message "Error for CPU 2: Unable to offline this CPU," you would enter the following `hwmgr` command:

```
# hwmgr -offline -name cpu2
```

For more information, see `codconfig`(8) and `hwmgr`(8)

The Manage CPUs SUITLET is available from the SysMan Menu and SysMan Station.

1.1.6.3 Hardware SCSI Bus Errors

SCSI CAM errors experienced by the Adaptec controller that require SCSI bus resets could cause PCI bus faults. These faults will be seen as a “Machine Check

System Uncorrectable" panic. This will require the system to be booted after the machine_check. A fix for this problem will be included in a future release

1.1.6.4 Compact Disk Drive Errors Logged

The TEAC CDR-W 416E drive that is shipped with the system will log errors on reboot if the CD-ROM media is not present. These messages are only informational.

1.1.6.5 Presence of Third-Party Devices May Cause System Panic

The ATM 3X-DAPBA-FA/UA driver may experience a panic on shutdown if third-party devices are installed.

1.1.6.6 Repeated Reboots May Cause Panic

Repeated reboots of the system may cause a kernel memory fault panic, but does not result in the loss of data. A reboot after the panic should be successful. A fix for this problem will be included in a future release.

1.1.6.7 Incorrect Free Page Counts Reported

The `vmstat -S` command reports incorrect free page counts on a sparsely configured system. A sparsely configured system is one that has gaps in the numbering of CPUs, for example 0, 1, 8,9 10,11.

1.1.6.8 USB Keyboard Driver Does Not Support Non-U.S. Locales

The USB keyboard driver does not support non-U.S. locales, and setting the system's language to anything other than 36 (U.S./English) causes the keyboard to be interpreted as a U.S./English keyboard anyway.

For example, on the Japanese keyboard with the SRM variable "language" set to 50 (Japanese JIS), Shift-2 produces a double quote (") character, while on the U.S./English keyboard it produces an ampersand (@). With this problem, keyboards set to Japanese will produce the ampersand.

A fix for this problem will be included in a future release.

1.1.7 Caution on Updating to Version 5.1B with DEGXA NICs

Do not attempt to do a update installation or rolling upgrade from Version 5.1A to Version 5.1B when the network device is a DEGXA-TA or DEGXA-SA and you have the Version 5.1A Patch Kit 4 and the New Hardware Devices V6 (NHD6) Kit installed.

The NHD6 and PK4 kits have provided fixes that are not in the base operating system release for Version 5.1B. Once the update is completed using another network device and the Version 5.1B Patch Kit 1 has been applied, the DEGXA network interface cards (NICs) can again be used for the network connection.

1.1.8 Tuning the NFS Server Duplicate Request Cache (Patch 494.00)

The NFS server maintains a list of recently completed non-repeatable requests. This list is used to reply to client retransmissions of the request in the event that the initial request transmission's reply was lost or that the server took too long to satisfy the request.

In some cases, under heavy NFS server load and over high aggregate network bandwidth involving changes to file systems (changes caused by the use of the `crate, link, unlink, mkdir, rmdir, truncate, utimes,` and `write` commands) problems may occur with the duplicate request cache. Thiese

problems can occur if all the elements in the duplicate request cache are cycled through between an initial client transmission and subsequent retransmission. If this occurs, the NFS server cannot detect that the retransmission is in fact a retransmission. This may result in the repetition of a request and may cause out of order writes or truncation and subsequent retruncation of a file.

Patch 494.00 provides a tuning variable to control the size of the NFS server's duplicate request cache:

- `nfs_dupcache_size` — Controls the absolute size of the NFS server duplicate request cache. This is measured in the number of elements that are allocated at NFS server initialization

If is determined that the size of the duplicate cache needs to be modified, you should change the `nfs_dupcache_size`. The new value for `nfs_dupcache_size`should be set to equal two times the value of `nfs_dupcache_entries`.

You must use the `dbx` command to modify `nfs_dupcache_size`. There is no sysconfig interface to this tuning variable.

1.2 Summary of Base Operating System Patches

This section provides descriptions of the patches in Patch Kit 1 for the Tru64 UNIX operating system.

Number: Patch 2.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 4.00

Abstract: Fixes premature termination of ofile kdbx extension

State: New

This patch fixes a premature termination of the ofile kdbx extension and warning messages in various kdbx extensions.

Number: Patch 6.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 8.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 10.00

Abstract: Correct potential buffer overflow

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the CDE online help. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.

Number: Patch 12.00

Abstract: Correct potential buffer overflow

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the CDE online help. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.

Number: Patch 14.00

Abstract: Fix for the dsfmgr utility

State: New

This patch fixes many small problems in dsfmgr.

Number: Patch 16.00

Abstract: Fix for the dsfmgr utility

State: New

This patch fixes many small problems in dsfmgr.

Number: Patch 18.00

Abstract: Security (SSRT2301, SSRT2275)

State: New

This patch:

- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the uucp utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.

Number: Patch 20.00

Abstract: Security (SSRT2301, SSRT2275)

State: New

This patch:

- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the uucp utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.

Number: Patch 30.00

Abstract: Allows auditing of login and su events

State: Supersedes Patches 25.00, 26.00, 27.00, 28.00

This patch:

- Allows the auditing of login and su events based in part on the contents of user profiles (for Enhanced Security), the prevailing auditing characteristics of the originating process, and the system-wide audit mask. Previously, only the system audit mask was referenced.
- Corrects a failure in the safe_open() routine that caused symbolic links given by a relative path from the current working directory sometimes to give ENOENT errors incorrectly.
- Corrects a potential floating point error in threaded applications.
- Fixes an extended regular expression problem where the interval expression {m,n} is handled incorrectly.
- Fixes a problem with SIA that caused the Internet Express LDAP Authentication module to be unable to look up default group information for a user at login time.

Number: Patch 33.00

Abstract: Correct potential buffer overflow

State: Supersedes Patch 31.00

This patch:

- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the DtSvc utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 36.00

Abstract: Correct potential buffer overflow

State: Supersedes Patch 34.00

This patch:

- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the DtSvc utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 38.00

Abstract: Adds new functionality to tcpdump

State: New

This patch adds support for IEEE 802.1Q Virtual Local Area Network (VLAN).

Number: Patch 42.00

Abstract: MD5 authentication problem with Version 2 RIP

State: New

This patch corrects a problem using MD5 authentication with Version 2 of the Routing Information Protocol (RIP).

Number: Patch 47.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 58.00

Abstract: Security (SSRT1-40U, SSRT1-41U, SSRT1-42U)

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 60.00

Abstract: Update to siacfg utility

State: New

On systems using Perl 5.8.0 and higher, this patch eliminates the "Using an array as a reference is deprecated" warning when running /usr/sbin/siacfg and during system boot.

Number: Patch 62.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 64.00

Abstract: Fix for find command

State: New

This patch fixes a problem with the find -ls command that caused it to display an incorrect number of blocks.

Number: Patch 84.00

Abstract: Security (SSRT2208)

State: New

This patch corrects a potential security vulnerability which may allow non-privileged users to gain unauthorized (root) access. This may be in the form of local and remote security domain risks.

Number: Patch 86.00

Abstract: Security (SSRT1-40U, SSRT1-41U, SSRT1-42U)

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 89.00

Abstract: Fixes defects in AutoFS user space and kernel code

State: Supersedes Patch 87.00

This patch:

- Fixes multiple defects in AutoFS user space and kernel code.
- Fixes a problem that prevents access to AutoFS file systems if ACLs are enabled.

Number: Patch 91.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 105.00

Abstract: Fix for tar command

State: New

This patch fixes a one byte gap/hole in the maximum file size in the tar command before an extended header record is used (8589934591 (octal 77777777777)).

Number: Patch 107.00

Abstract: Fix for X Server command line option

State: New

This patch fixes a problem where the X server's command line option to turn off VESA Display Power Management Signalling (-dpms) does not work.

Number: Patch 135.00

Abstract: Correct potential buffer overflow

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the dxterm utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.

Number: Patch 137.00

Abstract: Fix for startslip program

State: New

This patch fixes a problem with the startslip program that prevented it from extracting all information from the acucap file.

Number: Patch 139.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 143.00

Abstract: Fix race condition and improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 155.00

Abstract: Fix race condition and improper file access

State: Supersedes Patches 152.00, 153.00

This patch:

- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.
- Corrects a problem in which the sh command interpreter uses a high amount of CPU time.
- Fixes the problem that occurs while encoding "$@" in the Bourne shell.

Number: Patch 157.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 159.00

Abstract: Fix hwmgr command to show path state correctly

State: New

This patch fixes the hwmgr command to correctly show a path state.

Number: Patch 161.00

Abstract: Corrects cp performance problem

State: New

This patch:

- Corrects a cp command performance problem involving a change in the I/O buffer size from 64K to 8K.
- Corrects a problem in which the cp and cat commands produce different file sizes when reading from a tape device.

Number: Patch 167.00

Abstract: Security (SSRT2368, SSRT2368)

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper access.

Number: Patch 169.00

Abstract: Fix for SDLT media error

State: New

This patch adds the capability for KZPCA devices to work with SCSI devices that only support asynchronous data transfers and fixes SDLT media error caused bus resets.

Number: Patch 171.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 173.00

Abstract: Fix race condition and improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 176.00

Abstract: Resolves kernel memory faults in TCP/IP subsystem

State: Supersedes Patch 174.00

This patch resolves kernel memory faults in the TCP/IP subsystem.

Number: Patch 178.00

Abstract: Fix for lpd line printer daemon

State: New

Fixes the lpd deamon to correct /etc/hosts.lpd case sensitivity, for example, "node.domain" treated the same as "Node.Domain/"

Number: Patch 185.00

Abstract: Prevents addvol from adding invalid disks into domain

State: New

This patch prevents addvol from adding invalid disks into a domain.

Number: Patch 187.00

Abstract: Fix for invalid disks being added into domain

State: New

This patch prevents addvol from adding invalid disks into a domain.

Number: Patch 189.00

Abstract: Fix for rmtmpfiles script

State: New

This patch corrects a problem in which the rmtmpfiles script leave empty directories in /var/tmp at system startup.

Number: Patch 191.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 193.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 195.00

Abstract: Provides fixes for the collect utility

State: New

This patch fixes several problems with the collect utility and updates the utility from Version 2.0.0 to 2.0.5.

Number: Patch 197.00

Abstract: Read privileges being stripped from passwd file

State: New

This patch fixes a problem in which group and other read privileges get stripped from /etc/passwd when a user switches from enhanced to base security.

Number: Patch 199.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 201.00

Abstract: Fix for verify utility

State: New

This patch fixes a problem in which the verify utility core dumps if it encounters a specific type of metadata inconsistency.

Number: Patch 203.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 205.00

Abstract: Fixes a correctable error reporting problem

State: New

This patch fixes a correctable error reporting problem that turns off the reporting of correctable errors forever on any CPU, except CPU 0, once throttling of correctable errors has begun.

Number: Patch 207.00

Abstract: Correct potential buffer overflow

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the libXm utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.

Number: Patch 209.00

Abstract: Correct potential buffer overflow

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the libXm utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.

Number: Patch 219.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 221.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 223.00

Abstract: Add SCSI reserve/release support to mt

State: New

This patch adds SCSI reserve and release support to the mt program to assist open SAN tape management.

Number: Patch 225.00

Abstract: Interop problem between curses.h and esnmp.h.

State: New

This patch fixes an interoperability problem between the curses.h and esnmp.h header files.

Number: Patch 227.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 229.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 232.00

Abstract: Correct improper file access

State: Supersedes Patch 230.00

This patch:

- Adds support in script to remove all Persistant Reservations for MSA controller.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 234.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 238.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 240.00

Abstract: Fix for hwmgr command

State: New

Fixes a problem in which the display for the hwmgr -show name command is not aligned properly for the name field.

Number: Patch 248.00

Abstract: Fix for hwmgr delete command option

State: New

This patch fixes a problem where, when using hwmgr to delete a component, a "DELETE_COMMIT: Cannot fetch name." message may be displayed on the console. This problem can be seen frequently in a cluster environment when the component being deleted does not exist on the system.

Number: Patch 250.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 252.00

Abstract: Fix for audit_tool command

State: New

This patch fixes the audit_tool search algorithm to differentiate between prived and non-prived UIDs, and to allow regular expressions in string searches.

Number: Patch 254.00

Abstract: Correct improper file access

State: New

This patch:

- Corrects the problem of a core dump that occurs when the output from the lint program for a nonexistent file is supplied to error.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 256.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 258.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 260.00

Abstract: Code now prints greater than 61 UNIX domain sockets

State: New

This patch:

- Adds code to print greater than 61 UNIX domain sockets.
- Changes file read errors from /dev/kmem to ignore and continue in a running system.

Number: Patch 262.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 264.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 266.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 268.00

Abstract: Installs version V2.1-120 of libots3 libraries

State: New

This patch installs version V2.1-120 of /usr/lib/libots3.a and /usr/shlib/libots3.so, which fixes a problem where long-running OpenMP applications might overflow an internal libots3 counter, resulting in a breakdown of thread synchronization.

Number: Patch 270.00

Abstract: Installs version V2.1-120 of libots3 libraries

State: New

This patch installs version V2.1-120 of /usr/lib/libots3.a and /usr/shlib/libots3.so, which fixes a problem where long-running OpenMP applications might overflow an internal libots3 counter, resulting in a breakdown of thread synchronization.

Number: Patch 272.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 275.00

Abstract: Fix for hwmgr -view transaction -cluster command

State: Supersedes Patch 273.00

This patch:

- Corrects some command-parsing irregularities in hwmgr that may cause options like -category and -cluster to be confused.
- Corrects a problem in which information from the hwmgr -view transaction -cluster command for a node on a cluster may not be displayed.

Number: Patch 464.00

Abstract: Correct improper file access

State: Supersedes Patch 277.00

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 279.00

Abstract: Corrections to Oxygen VX1 graphics card XCopyPlane

State: New

Corrects a problem with the Oxygen VX1 graphics card to make XCopyPlane copy only the requested bitplane rather than all bitplanes.

Number: Patch 281.00

Abstract: Fixes a problem in usb_hid.mod

State: New

Corrects a problem in which a kernel memory fault sometimes occurs if a USB keyboard or mouse does not respond quickly enough. This KMF can occur during boot or soon after a USB keyboard or mouse is connected. Any device can trigger this, though it is neither predictable nor common.

Number: Patch 283.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 285.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 287.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 289.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability which, under certain circumstances, could compromise system integrity.

Number: Patch 294.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 296.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 298.00

Abstract: Fixes consvar -s bootdef_dev failure with KZPCC

State: New

This patch fixes consvar -s bootdef_dev failure with KZPCC.

Number: Patch 300.00

Abstract: Login process crashes when LDAP users try to log in

State: New

This patch fixes a problem in with the login process may crash when LDAP users or users belonging to an LDAP group attempt to log in.

Number: Patch 304.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 306.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 309.00

Abstract: Performance tool failures on Sierra Cluster (PFS)

State: Supersedes Patch 307.00

This patch:

- Fixes a problem in which the prof -pixie -testcoverage <exe> <exe>.Counts sometimes reports invalid source line number ranges.
- Fixes performance tool failures on Sierra Clusters Parallel File Systems (PFS) .

Number: Patch 311.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 313.00

Abstract: Correct improper file access

State: New

This patch:

- Corrects a potential security vulnerability where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.
- Addresses a problem in which performing a sort on a large database using numerous keys fails during the consolidation phase of the temporary files.

Number: Patch 317.00

Abstract: Security (SSRT1-40U, SSRT1-41U, SSRT1-42U)

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 320.00

Abstract: Fixes problem with IPv6 neighbor discovery daemon

State: Supersedes Patch 318.00

This patch:

- Fixes a regression in the operation of the IPv6 neighbor discovery daemon, where IPv6 addresses will not be automatically configured on PPP interfaces.
- Fixes a problem with IPv6 neighbor discovery daemon, where under certain circumstances, the daemon can cause bad information to be written to a DNS database, thereby causing failures on subsequent database reloads.

Number: Patch 322.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 324.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 326.00

Abstract: Fixes a linker error

State: New

This patch fixes a linker error that occurs when running the command ld -update_registry /dev/null.

Number: Patch 328.00

Abstract: Fixes and improves the mcutil program

State: New

This patch fixes and improves the mcutil program by correcting how bus resets are handled by the program and enhancing its error reporting capabilities.

Number: Patch 330.00

Abstract: Allows evmd to stop listening on default TCP port 619

State: New

This patch allows the Event Manager daemon, evmd, to stop listening on its default TCP port 619. This capability is not available for clustered systems.

Number: Patch 332.00

Abstract: Fixes memory leak in the PanoramiX/Xinerama Extension

State: New

This patch fixes a memory leak in the PanoramiX/Xinerama Extension that could cause a process core dump.

Number: Patch 334.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 339.00

Abstract: Updated keyboard map for Russian 3R-LKQ48-BT

State: New

This patch provides an updated keyboard map for the Russian 3R-LKQ48-BT keyboard model.

Number: Patch 343.00

Abstract: Fixes problem seen with TAHI IPv6 conformance test

State: New

This patch fixes a problem seen with the TAHI IPv6 conformance test, specifically Test 4 for the IPv6 Specification.

Number: Patch 345.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 347.00

Abstract: Fix allows fuser to display the reference flag

State: New

This patch allows the fuser utility to display the reference flag, which indicates the type of reference made; for example, open, closed, unlinked, or mmapped.

Number: Patch 349.00

Abstract: Corrections to several problems in fixfdmn

State: New

This patch corrects several problems with the fixfdmn utility.

Number: Patch 351.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 356.00

Abstract: Fix for ftp open command

State: Supersedes Patch 354.00

This patch:

- Corrects a bug in the ftp open command. The optional port argument now accepts port numbers between 32768 and 65535.
- Corrects a potential security vulnerability which, under certain circumstances, could compromise system integrity.

Number: Patch 358.00

Abstract: Fix for mountd daemon

State: New

This patch enables mountd to correctly handle entries with multiple lines input in exports file.

Number: Patch 360.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 362.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 364.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 366.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 368.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 370.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 372.00

Abstract: Security (SSRT1-40U, SSRT1-41U, SSRT1-42U)

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 378.00

Abstract: Security (SSRT1-40U, SSRT1-41U, SSRT1-42U)

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 380.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 384.00

Abstract: Fix for telnetd daemon

State: New

Fixes a problem in which telnetting from some machines (MS), will leave a UDP port open, requiring a call to yp_unbind() after getnameinfo() to close all ports.

Number: Patch 387.00

Abstract: Correct improper file access

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 389.00

Abstract: Update SSH Tru64 UNIX V1.1 (2.4.1) to SSH 3.2

State: New

This patch addresses several issues and problems with the SSH program, including interoperability with other SSH implementations, SSH client/server configuration files compatibility issues, and the lack of IPV6 support.

Number: Patch 391.00

Abstract: Updates reference pages for VLAN functionality

State: New

This patch revises the ifconfig(8), lan_config(8), niffconfig(8), ping(8), vlanconfig(8), and vlan(7) reference pages for VLAN functionality.

Number: Patch 394.00

Abstract: Correct improper file access

State: Supersedes Patches 335.00, 337.00, 392.00

This patch:

- Fixes several potential security vulnerabilities which, under certain circumstances, could compromise system integrity. These may be in the form of improper file access.
- Fixes a problem in which the volmigrate command returns a shell error when attempting to migrate an AdvFS domain with multiple filesets. With this fix, these domains can be migrated if all the filesets are mounted.
- Prevents inconsistent LSM volumes when the name of a partition that is being encapsulated matches the name of a current LSM volume.

Number: Patch 396.00

Abstract: Fix for ldapcd daemon

State: Supersedes Patch 56.00

This patch fixes the following problems with the ldapcd daemon:

- It may crash when resolving group codes with very large GIDs.
- It may crash when the LDAP Directory Server is unavailable.
- It prevents LDAP users from being authenticated, even when they are providing the correct password.

Number: Patch 414.00

Abstract: Revises several SSH reference pages

State: New

This patch revises several of the SSH reference pages which address several issues and problems with SSH, including the following:

- Interoperability with other SSH implementations
- Client/server configuration files compatibility issues
- The lack of IPV6 support

Number: Patch 416.00

Abstract: Fix for creacct hang

State: New

Fixes a problem that causes the creacct command to hang when the W2K Active Directory is misconfigured.

Number: Patch 421.00

Abstract: Revises envconfig.8 and envmond.8 reference pages

State: New

This patch revises the envconfig(8) and envmond(8) reference pages for the environmental monitoring facilities /usr/sbin/envmond and /usr/sbin/envconfig to support the new GS1280 hardware platform.

Number: Patch 423.00

Abstract: Fix potential denial of service

State: New

This patch corrects a potential security vulnerability for systems using Internet Protocol Security (IPsec). Under certain circumstances, a remote attacker may be able to cause IPsec to block all IP traffic from the system, creating a denial of service.

Number: Patch 425.00

Abstract: NHD6 installs failed to see new disk information

State: New

This patch updates ddr.mod to support new hardware (NHD6) devices.

Number: Patch 427.00

Abstract: Security (SSRT2266)

State: Supersedes Patches 179.00, 180.00, 181.00, 183.00

This patch:

- Corrects a potential security that may result in denial of service. This may be in the form of local and remote security domain risks. The following potential security vulnerability has been corrected:

  SSRT2266 IGMP (Severity - High) which, under certain circumstances, could compromise system integrity.

- Fixes a problem in the kernel network subsystem that causes a kernel memory fault panic in the m_adj() routine.
- Fixes a problem in the IP multicast loopback code that causes a kernel memory fault panic.
- Fixes a problem in which the kernel incorrectly closes a socket, thereby causing Sybase 1613 errors to be produced.
- Fixes a problem in which a duplicate IP address might be configured on the system, or an IP address might be configured with an incorrect netmask.

Number: Patch 429.00

Abstract: Security (SSRT0711U)

State: New

This patch:

- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.
- Corrects a problem in which crontab removes its entries and the vi editor truncates an existing file when a file system is full.

Number: Patch 431.00

Abstract: Provides support functionality for DS20L platform

State: Supersedes Patches 214.00, 215.00, 217.00

This patch:

- Fixes a problem that can cause an AlphaServer ES45 system to hang if the Xserver is restarted or the system rebooted without a power cycle when using the Radeon AGP graphics device.
- Prevents the memory troller from starting on AlphaServer systems with aluminum ev68 CPUs.
- Fixes several IPMI-related problems, including the following:
  - Erroneous fields in 686 OS-detected environmental machine check logout frame
  - Unusually large number of 686 sensor timeouts with heavy system load
  - IPMI always reporting -48v sensors as broken, seen as "redundant power supply failed" messages
  - An IPMI memory leak
- Provides additional environmental support functionality for the AlphaServer DS20L system.

Number: Patch 433.00

Abstract: Fix race condition and improper file access

State: Supersedes Patch 236.00

This patch:

- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.
- Corrects a problem in which a core dump may occur when using the csh shell from the Japanese locale.
- Fixes the problem with csh shell redirection that occurs while using a tilde (~) operation to redirect standard input and standard output of a command to a file residing in the home directory.

Number: Patch 438.00

Abstract: Additional support for Ultrium 2 SCSI tape drive

State: Supersedes Patches 290.00, 292.00, 436.00

This patch:

- Provides support for the SDLT160/320 and Ultrium 2 SCSI tape drives, including support for the Ultrium 2 SCSI to rewind after a reset behavior.
- Ensures proper compilation of the DDR database.

Number: Patch 440.00

Abstract: Fix for kernel memory fault

State: New

This patch fixes the problem of a kernel memory fault in systems that contain more than eight IDE/ATA buses.

Number: Patch 442.00

Abstract: Incorrect I/O status may be returned by KZPEA driver

State: Supersedes Patch 315.00

This patch:

- Corrects problems in the aha_chim driver that could result in bus hangs, panics, and inappropriate access of freed memory during high rate of bus resets.
- Corrects a problem in which Incorrect I/O status may be returned by the KZPEA driver when attempting to abort an I/O during a reset.

Number: Patch 444.00

Abstract: Revises tcpdump.8 ref page for VLAN functionality

State: New

This patch revises the tcpdump(8) reference page for virtual local area network (VLAN) functionality.

Number: Patch 446.00

Abstract: Revises the mt.1 reference page

State: New

This patch revises the mt(1) reference page for the mt command, which has three new commands, mt reserve, mt release and mt tur.

Number: Patch 448.00

Abstract: Allows multiple VX1 graphic cards to be configured

State: Supersedes Patch 353.00

This patch:

- Corrects a problem in which systems configured with VX1 graphics card will not return to console when the halt button is pressed, thereby making the console unusable.
- Allows multiple VX1 graphic cards to be configured in a separate I/O box system.

Number: Patch 450.00

Abstract: Fix for smsd triggering LSM configuration errors

State: New

This patch corrects a problem in which the SysMan Station daemon, esmsd, triggers LSM configuration errors when querying LSM in a cluster. The installation of this patch ensures that a cluster member will be up-to-date with respect to the LSM configuration when calls are made to an internal LSM routine.

Number: Patch 452.00

Abstract: Modifications for environmental monitoring facilities

State: Supersedes Patch 40.00

This patch:

- Modifies the environmental monitoring facilities /usr/sbin/envmond and /usr/sbin/envconfig to support the AlphaServer GS1280 system.
- Updates the environmental monitoring daemon envmond to ensure the correct EVM events are being sent at the correct time.

Number: Patch 454.00

Abstract: Correct potential buffer overflow

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the dxsysinfo utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.

Number: Patch 456.00

Abstract: Fix buffer overflow and improper file access

State: Supersedes Patch 246.00

This patch:

- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 458.00

Abstract: Correct potential buffer overflow

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 460.00

Abstract: Correct potential buffer overflow

State: New

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management.

Number: Patch 462.00

Abstract: Support for SmartArray disk controllers

State: New

Adds Support for SmartArray disk controllers. In the absence of this support, the SysMan Station hardware view fails to operate if the SmartArray product is installed on the system.

Number: Patch 478.00

Abstract: Installs DECthreads V3.20-029c

State: Supersedes Patch 22.00

This patch installs DECthreads V3.20-029c, which fixes problems that may affect threaded programs, including a problem with floating point data corruption. This version of DECthreads is the initial support version of the HP POSIX Threads Library for Tru64 UNIX V5.1B.

Number: Patch 480.00

Abstract: Installs DECthreads V3.20-029c

State: Supersedes Patch 24.00

This patch installs DECthreads V3.20-029c, which fixes problems that may affect threaded programs, including a problem with floating point data corruption. This version of DECthreads is the initial support version of the HP POSIX Threads Library for Tru64 UNIX V5.1B.

Number: Patch 484.00

Abstract: Corrects invalid hwmgr show component inconsistency

State: Supersedes Patches 144.00, 145.00, 146.00, 147.00, 148.00, 149.00, 151.00

This patch:

- Fixes a problem in which when reboooting immediately after entering a hwmgr -redirect SCSI command you will boot to single user mode with the following error being displayed: “bcheckrc: Device Naming failed boot configure or verify Please correct the problem and continue or reboot INIT: SINGLE-USER MODE.”
- Fixes a problem in which when using the hardware manager to show attributes, the LONG_MAX and LONG_MIN values are displayed incorrectly.
- Corrects a problem that causes the system to hang when mounting cluster root if the cluster root domain devices are private to different cluster members. This fix allows the cluster to boot with a warning to the console. Although this configuration is not recommended, it should not make the cluster unbootable. The situation involves non-LSM cluster root domains.
- Introduces the type checking of attributes when registering components with the hardware manager.
- Corrects a potential deadlock in the hardware configuration subsystem.
- Prevents the hardware management cluster database from being reset.
- Corrects an invalid hwmgr show component inconsistency.
- Corrects a problem that occurs during environmental testing. When using the hwmgr utility to verify that a particular sensor’s status would change from OK to Fault, each time the state changed and hwmgr requested the new value, hwmgr dumped core.

Number: Patch 486.00

Abstract: Security (SSRT0785U)

State: Supersedes Patches 162.00, 163.00, 165.00

This patch:

- Corrects the following problems with the account management tools:
  - The userdel command possibly core dumping when the shell field is empty in the passwd file.
  - The usermod command not working as expected with NIS +/- users.
  - The useradd command not managing default and template data properly. This showed up most notably with the useradd -p command producing the message "Password must be between 32 and 80 characters."
  - Several other minor problems.
- Updates the account management tools to use the latest versions of the ASU (Advanced Server for UNIX) API calls when ASU is in use on the server.
- Fixes a number of problems with the Account Manager application, dxaccounts, on a system with ASU installed.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of passwords that have a length outside of the intended range.

Number: Patch 490.00

Abstract: Fix process management

State: Supersedes Patches 213.00, 108.00, 109.00, 110.00, 111.00, 112.00, 113.00, 114.00, 115.00, 116.00, 117.00, 118.00, 119.00, 120.00, 121.00, 122.00, 123.00, 124.00, 125.00, 126.00, 127.00, 128.00, 129.00, 130.00, 131.00, 133.00, 397.00, 398.00, 399.00, 400.00, 401.00, 402.00, 403.00, 405.00

This patch:

- Fixes a system hang when using Open3D over the AGP bus on a GS1280.
- Corrects performance issues when accessing a file with direct I/O enabled.
- Fixes an AdvFS asynchronous direct I/O problem that could cause a thread to hang.
- Fixes a problem encountered where a truncated AdvFS file erroneously zeroed data for the remaining leading segment of the file.
- Changes the behavior of migrate_normal and migrate_stripe when migrating an original file that has a clone. If the clone was marked out of sync, migrate could come back with E_CLONE_OUT_OF_SYNC even though the migrate succeeded. Now this case is caught, and handled.
- Replaces the system panics caused by "Can't clear bit twice" with a domain panic.
- Fixes a problem in which a crash occur when an AdvFS file system reports I/O errors and enters into a domain panic state. AdvFS's error cleanup would panic on an invalid pointer and report an "invalid memory read access from kernel mode" panic message.
- Fixes an issue encountered in configurations where the primary processor is not the first processor within a rad.
- Resolves a problem of not being able to view files on some CD-ROM media that is created by third party software and corrects the erroneous reporting of success when attempting to write beyond the file size limit using synchronized I/O and the calculation of _PC_FILESIZEBITS, which is used by the operating system for pathconf file characteristics.
- Fixes a problem with audit data not being displayed by the audit tool,
- Fixes problems with file object selection and deselection and directories.
- Fixes problems with NUMA performance associated with auditing.
- Fixes a race during AdvFS volume removal that can cause a panic in the bs_osf_complete() routine.
- Fixes a problem with kernel memory fault in shadowvnode() caused by NULL vnode pointer.
- Fixes insmntque() to conform to proper locking when removing and adding vnode to the mount vlist.
- Fixes a problem with excessive FIDS_LOCK contention observed when large numbers of files are using system based file locking.
- Corrects the AdvFS system call OP_GET_BKUP_XTNT_MA to avoid a silent infinite loop in vdump. The call will now return the valid xtntCnt when it fails due to E_NOT_ENOUGH_XTNTS.
- Fixes a panic caused by a problem within the swapping subsystem.
- Fixes mount and umount failures and panics in MFS, UFS, and FDFS.
- Fixes an AdvFS alignment fault panic caused by inconsistent AdvFS metadata in a directory. In particular, the directory's entry size is an unaligned value.
- Corrects a potential problem with modifying files via direct I/O when there is a clone fileset.
- Fixes a panic within the two-level scheduling subsystem.

Patch 490.00 Continued

- Improves AdvFS informational messages as follows:
  - Advscan reports if a domain has all of its volumes, but they are stored in a different directories. This scenario will cause mount to fail.
  - The AdvFS I/O error message includes the location of a file that will help users to translate the error number into an error message.
- Forces a domain panic instead of a system panic if AdvFS metadata is discovered to be incorrect in frag_group_dealloc.
- Fixes a part of AdvFS migration code in order to prevent the rmvol utility's "Can't remove volume" error.
- Fixes a problem when monitoring I/O using the advfsstat command.
- Fixes a rare problem that causes thread blocking when waiting for memory.
- Fixes a problem in which a domain panic may occur in idx_lookup_node_int or bs_frag_dealloc under heavy file system activity, generating one of the following messages:

  idx_lookup_node_int: bs_refpg failed
  bs_frag_dealloc: rbf_pinpg (4) failed, return code = -1035

- Fixes a problem in which the fuser utility is unable to report on all referenced resources, which occurs when attempting to identify reasons for unmount failures.
- Improves the process exit procedure for processes that have had the nice command used on them.
- Corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.
- Corrects a race condition in AdvFS in which it avoids a potential stranded log record in memory that does not get out to disk.
- Fixes an rmvol E_PAGE_NOT_MAPPED error.
- Eliminates an ENO_MORE_BLKS error seen when performing a copy on write (COW) procedure to a clone file while an rmvol operation is in progress.
- Fixes a problem in which a system on a cluster can panic with the message "ics_unable_to_make_progress: input thread stalled."
- Adds support for CPU indictment on AlphaServer ES80 and GS1280 systems.
- Adds support in the platform code to handle MSI capable adapters. AlphaServer GS1280 systems support option cards that require MSI capabilities
- Adds support to get live status information for air movers and power supplies on AlphaServer ES80 and GS1280 systems and to log intrusion packets to the error log.
- Fixes a problem in which a process waiting on a semaphore does not get woken up.
- Fixes a problem in which the extension of UNIX file systems via the mount command can effectively disable the use of the file system.
- Fixes a problem on some LSM based systems in which a panic can occurs after a file system extension has been completed.
- Fixes a problem in which a hang may occur when a rmvol operation is performed after a cluster node failure during volmigrate, volunmigrate, or frag file migration.
- Corrects a locking problem with NFS running over UFS.
- Fixes an obliteration of user file information, which is most often seen after using the ftruncate() function.

Number: Patch 492.00

Abstract: Correct improper file access

State: Supersedes Patch 77.00

This patch corrects a potential security vulnerability where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access.

Number: Patch 494.00

Abstract: Fixes an NFS client panic

State: Supersedes Patches 78.00, 79.00, 80.00, 82.00, 341.00, 409.00, 410.00, 412.00, 482.00

This patch:

- Fixes two potential problems in the NFS V3 client where unstable writes could potentially remain uncommitted when they should have been committed to stable storage.
- Eliminates a false directory lookup warning message generated by an incorrect comparison caused by mismatched fileid variable types.
- Improves client caching performance.
- Fixes a problem that can cause a system crash when an NFS server exports files on a third party file system (that is, one not built into Tru64 UNIX).
- Prevents the loss of a single system image for an NFS file system mounted from a cluster, as a result of problems communicating with the external NFS server.
- Fixes a memory leak in the NFS server when it receives malformed packets.
- Allows the size of the NFS server's duplicate request cache to be adjusted as needed.
- Fixes a problem in which a Tru64 UNIX NFS client panics when it receives a null entry as a response to a readdirplus request from an NFS server.
- Fixes a problem in which a Tru64 NFS UNIX client panics as a result of receiving illegal file access mode from an NFS client.
- Increases TCP windows from 96 KB to 500 KB to improve performance.
- Causes the netisr thread to dynamically estimate the reply size and subsequently reserve the space in the socket buffer.
- Adds a new timeout check to notice when data in a socket buffer has not been acknowledged in 30-50 seconds and copies those buffers to allow the UBC to free up those mbufs.
- Addresses the following problems with the NFS server:
  - A flaw that could cause it to crash upon reception of malformed input.
  - A flaw that could cause it to crash with concurrent read and truncate on an AdvFS file.
  - A flaw that could cause it to crash with malformed or malicious READDIR[PLUS] version 3 RPCs.

Number: Patch 496.00

Abstract: Provides the V1.07 release of ciss driver

State: Supersedes Patches 92.00, 93.00, 94.00, 95.00, 96.00, 97.00, 98.00, 99.00, 100.00, 101.00, 374.00, 103.00, 417.00, 419.00

This patch:

- Fixes a problem with the Smart Array driver that could cause a system hang to occur during error recovery when I/O is active.
- Adds support for new EVM events to be generated by the Event Monitoring daemon, /usr/sbin/envmond.
- Fixes the system panic "PWS_CCB_QUE_REMOVE: ccb not on any list," caused by a device or bus reset occurring during the execution of a command to a media changer device, like a tape library.
- Corrects a problem that causes a system panic while running applications performing open of RAID device, and the faulting routine was control_port_open.
- Adds an event to indicate that the soft or hard error count has changed on the device identified in the event.
- Fixes a situation in which mounting a valid CD-ROM for the first time fails with the message “No valid file system exists on this partition,” although subsequent mounts of the same CD-ROM work fine.
- Provides a configurable setting that causes an error return for any read of tape from a tape that requests less than the full amount of data in the tape block.
- Enables SmartArray 5300 controller hardware events to be logged to binary.errlog during a boot. This is useful in diagnosing logical volume state change and physical drive hotswaps that can occur while the system is not booted.
- Corrects a problem in which /sbin/ddr_config does not accept values for ReadyTimeSeconds larger than 255. The new limit is 86400 seconds (24 hours).
- Fixes problems with NUMA disk statistics.
- Fixes a KMF problem that can occur when some nodes in cluster are rebooted and a device is shared by all the nodes.
- Changes the CAM subsystem message that is printed to the error log on a recovered read error from "bad block number" to "block number."
- Corrects a problem in which camreport may report negative device IDs.
- Fixes the reporting to the binary errlog of device monitoring events and hardware errors during disk recovery from the disk driver.
- Corrects a problem with hwmgr utility deletes while a SCSI scan is in progress.
- Corrects a problem in which a path event can cause hang in cdisk_online during disk open of HSG80.
- Installs the V1.07 release of the ciss driver, which is the mandatory minimum version to support the Smart Array 5300 Controller.
- Address an issue in which AdvFS domain panics occur during HSZ and HSG failovers

Number: Patch 498.00

Abstract: Improve I/O performance by reducing kernel locking overhead.hubs

State: Supersedes Patches 65.00, 66.00, 67.00, 68.00, 69.00, 70.00, 71.00, 72.00, 73.00, 75.00, 376.00, 406.00, 408.00, 241.00, 242.00, 244.00, 435.00, 488.00

- Fixes a process hang condition.
- Fixes a "thread_block: simple lock held" panic.
- Corrects a situation in which a system could panic during a particular machine check.
- Corrects several problems of 3D client hangs when using a Radeon graphics card.
- Fixes a performance problem seen when doing wiring on gh_chunks memory; for example, an Oracle application.
- Protects against "get_color_bucket: empty buckets!" panics and "kernel memory fault" failures on systems with mixed cache parameters.
- Fixes a kernel memory fault in u_seg_global_destroy.
- Corrects a kernel memory fault that can happen when running applications that use the Cray Intra-Node Shared Memory library.
- Prevents a potential process (not system) hang seen when a system comes under heavy memory load with monolithic memory use (gigabyte-scale single objects).
- Prevents a kernel memory fault when running with protection on the 128-byte bucket. (This should only be running with this as directed by support personnel.)
- Corrects a situation in which a taso-compiled binary is unable to allocate more memory after performing a series of mmap calls.
- Fixes an occasional panic that can be seen when reading from a process using Granularity Hints via the /proc file system.
- Fixes a panic that generates the message “u_seg_vop_remove: seg not found in vop.”
- Fixes a situation in which mmap memory locked with mlockall() using the MCL_FUTURE flag does not become wired automatically.
- Fixes a "Bigpage Assertion Failed" panic.
- Corrects a rounding error for vm attribute vm_bigpg_thresh.
- Corrects the handling of bad pages when bigpages are enabled.
- Fixes "page mapped" panics when using the mmap() function for dev/mem to access free bigpages.
- Corrects a condition that causes a delete_pv_entry panic when kernel virtual-address space has high usage.
- Fixes a problem seen when USB hubs (or any other bus device) are removed from a running system.
- Removes a restriction in which dynamic VMEbus device drivers could only probe one controller per driver. With this patch, multiple controllers per driver can be configured successfully.
- Fixes a potential floating point register corruption.
- Fixes multiple problems affecting a system with peripheral USB hubs attached, as well as problems that might occur when moving or adding USB host adapters.
- Improves I/O performance by reducing kernel locking overhead.

Number: Patch 500.00

Abstract: Adds new functionality to support IEEE 802.1Q

State: Supersedes Patches 43.00, 45.00, 48.00, 49.00, 50.00, 51.00, 52.00, 54.00

This patch:

- Adds IEEE 802.1Q Virtual Local Area Network (VLAN) support for :
  - DEGPA
  - DEGXA
  - DE50x, lan_common.h
  - DE60x
- Adds support to the ifconfig application for the IPv6 command line argument ip6reachabletime.
- Adds support for Ethernet adapters, including the DS25 onboard 10/100/1000 port, and does the following:
  - Fixes a problem in the alt driver for DEGPA Gigabit Ethernet adapters. This problem affects all Tru64 systems containing DEGPA network interfaces.
  - Fixes numerous issues in the driver for DEGXA Gigabit Ethernet adapters.

2

TruCluster Patches

This chapter provides information about the patches included in Patch Kit 1 for the TruCluster Server software.

This chapter is organized as follows:

- Section 2.1 provides release notes that are specific to the TruCluster Server software patches in this kit.
- Section 2.2 provides brief descriptions of the TruCluster Server patches included in this kit.

2.1 Release Notes

This section provides release notes that are specific to the TruCluster Server software patches in this kit.

2.1.1 Required Storage Space

The following storage space is required to install the base and TruCluster Server components of this patch kit:

- Approximately 250 MB of temporary storage space is required to untar this patch kit (base and TruCluster). We recommend that this kit not be placed in the `/`, `/usr`, or `/var` file systems because doing so may unduly constrain the available storage space for the patching activity.
- Approximately 59 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.
- Approximately 59 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.
- Approximately 644 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.
- Approximately 184 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

See Section 1.1.1 for information on space needed for the operating system patches.

2.1.2 AlphaServer ES47 or AlphaServer GS1280 Hangs When Added to Cluster

If after running `clu_add_member` to add an AlphaServer ES47 or AlphaServer GS1280 as a member of a TruCluster the AlphaServer hangs during its first boot, try rebooting it with the original V5.1B generic cluster kernel, `clu_genvmunix`.

Use the following instructions to extract and copy the V5.1B cluster `genvmunix` from your original Tru64 UNIX kit to your AlphaServer ES47 or AlphaServer GS1280 system. In these instructions, the AlphaServer ES47 or AlphaServer

GS1280 is designated as member 5. Substitute the appropriate member number for your cluster.

1. Insert the Tru64 UNIX Associated Products Disk 2 into the CD-ROM drive of an active member.
2. Mount the CD-ROM to `/mnt`. For example:

```
# mount -r /dev/disk/cdrom0c /mnt
```

3. Mount the bootdisk of the AlphaServer ES47 or AlphaServer GS1280 on its specific mount point; for example:

```
# mount root5_domain#root /cluster/members/member5/boot_partition
```

4. Extract the original `clu_genvmunix` from the CD-ROM and copy it to the bootdisk of the AlphaServer ES47 or AlphaServer GS1280 member.

```
# zcat < TCRBASE540 | ( cd /cluster/admin/tmp; tar -xf -
./usr/opt/TruCluster/clu_genvmunix)
# cp /cluster/admin/tmp/usr/opt/TruCluster/clu_genvmunix \
/cluster/members/member?/boot_partition/genvmunix
# rm /cluster/admin/tmp/usr/opt/TruCluster/clu_genvmunix
```

5. Unmount the CD-ROM and the bootdisk:

```
# umount /mnt
# umount /cluster/members/member5/boot_partition
```

6. Reboot the AlphaServer ES47 or AlphaServer GS1280

2.1.3 Updates for Rolling Upgrade Procedures

The following sections provide information on rolling upgrade procedures.

2.1.3.1 Unrecoverable Failure Procedure

The procedure to follow if you encounter unrecoverable failures while running `dupatch` during a rolling upgrade has changed. The new procedure calls for you to run the `clu_upgrade -undo install` command and then set the system baseline. The procedure is explained in the *Patch Kit Installation Instructions* as notes in Section 5.3 and Section 5.6.

2.1.3.2 During Rolling Patch, Do Not Add or Delete OSF, TCR, IOS, or OSH Subsets

During a rolling upgrade, do not use the `/usr/sbin/setld` command to add or delete any of the following subsets:

- Base Operating System subsets (those with the prefix `OSF`).
- TruCluster Server subsets (those with the prefix `TCR`).
- Worldwide Language Support (WLS) subsets (those with the prefix `IOS`).
- New Hardware Delivery (NHD) subsets (those with the prefix `OSH`).

Adding or deleting these subsets during a roll creates inconsistencies in the tagged files.

2.1.3.3 Undoing a Rolling Patch

When you undo the stages of a rolling upgrade, the stages must be undone in the correct order. However, the `clu_upgrade` command incorrectly allows a user undoing the stages of a rolling patch to run the `clu_upgrade undo preinstall` command before running the `clu_upgrade undo install` command.

The problem is that in the install stage, `clu_upgrade` cannot tell from the `dupatch` flag files whether the roll is going forward or backward. This ambiguity allows a

user who is undoing a rolling patch to run the `clu_upgrade undo preinstall` command without first having run the `clu_upgrade undo install` command.

To avoid this problem when undoing the stages of a rolling patch, make sure to follow the documented procedure and undo the stages in order.

2.1.3.4 Ignore Message About Missing ladebug.cat File During Rolling Upgrade

When installing the patch kit during a rolling upgrade, you may see the following error and warning messages. You can ignore these messages and continue with the rolling upgrade.

```
Creating tagged files.

.....................................................................
.....

*** Error ***
The tar commands used to create tagged files in the '/usr' file system have
reported the following errors and warnings:
     tar: lib/nls/msg/en_US.88591/ladebug.cat : No such file or directory
.....................................................

*** Warning ***
The above errors were detected during the cluster upgrade. If you believe that
the errors are not critical to system operation, you can choose to continue.
If you are unsure, you should check the cluster upgrade log and refer
to clu_upgrade(8) before continuing with the upgrade.
```

2.1.3.5 clu_upgrade undo of Install Stage Can Result in Incorrect File Permissions

This note applies only when both of the following are true:

- You are using `installupdate`, `dupatch`, or `nhd_install` to perform a rolling upgrade.
- You need to undo the `install` stage; that is, to use the `clu_upgrade undo install` command.

In this situation, incorrect file permissions can be set for files on the lead member. This can result in the failure of `rsh`, `rlogin`, and other commands that assume user IDs or identities by means of `setuid`.

The `clu_upgrade undo install` command must be run from a nonlead member that has access to the lead member's boot disk. After the command completes, follow these steps:

1. Boot the lead member to single-user mode.
2. Run the following script:

```
#!/usr/bin/ksh -p
#
#    Script for restoring installed permissions
#
cd /
for i in /usr/.smdb./$(OSF|TCR|IOS|OSH)*.sts
do
  grep -q "_INSTALLED" $i 2>/dev/null && /usr/lbin/fverify -y <"${i%.sts}.inv"
done
```

3. Rerun `installupdate`, `dupatch`, or `nhd_install`, whichever is appropriate, and complete the rolling upgrade.

For information about rolling upgrades, see Chapter 7 of the *Cluster Installation* manual, `installupdate`(8), and `clu_upgrade`(8).

2.1.3.6 Missing Entry Messages Can Be Ignored During Rolling Patch

During the `setup` stage of a rolling patch, you might see a message like the following:

```
Creating tagged files.
...................................................................

clubase: Entry not found in /cluster/admin/tmp/stanza.stdin.597530

clubase: Entry not found in /cluster/admin/tmp/stanza.stdin.597568
```

An `Entry not found` message will appear once for each member in the cluster. The number in the message corresponds to a PID.

You can safely ignore this `Entry not found` message.

2.1.3.7 Relocating AutoFS During a Rolling Upgrade on a Cluster

This note applies only to performing rolling upgrades on cluster systems that use AutoFS.

During a cluster rolling upgrade, each cluster member is singly halted and rebooted several times. The *Patch Kit Installation Instructions* direct you to manually relocate applications under the control of Cluster Application Availability (CAA) prior to halting a member on which CAA applications run.

Depending on the amount of NFS traffic, the manual relocation of AutoFS may sometimes fail. Failure is most likely to occur when NFS traffic is heavy. The following procedure avoids that problem.

At the start of the rolling upgrade procedure, use the `caa_stat` command to learn which member is running AutoFS. For example:

```
# caa_stat -t
Name            Type           Target    State     Host
------------------------------------------------------------
autofs          application    ONLINE    ONLINE    rye
cluster_lockd   application    ONLINE    ONLINE    rye
clustercron     application    ONLINE    ONLINE    swiss
dhcp            application    ONLINE    ONLINE    swiss
named           application    ONLINE    ONLINE    rye
```

To minimize your effort in the procedure described as follows, it is desirable to perform the roll stage last on the member where AutoFS runs.

When it comes time to perform a manual relocation on a member where AutoFS is running, follow these steps:

1. Stop AutoFS by entering the following command on the member where AutoFS runs:

   ```
   # /usr/sbin/caa_stop -f autofs
   ```

2. Perform the manual relocation of other applications running on that member:

   ```
   # /usr/sbin/caa_relocate -s current_member -c target_member
   ```

After the member that had been running AutoFS has been halted as part of the rolling upgrade procedure, restart AutoFS on a member that is still up. (If this is the roll stage and the halted member is not the last member to be rolled, you can minimize your effort by restarting AutoFS on the member you plan to roll last.)

1. On a member that is up, enter the following command to restart AutoFS. (The member where AutoFS is to run, *target_member*, must be up and running in multi-user mode.)

   ```
   # /usr/sbin/caa_startautofs -c target_member
   ```

2. Continue with the rolling upgrade procedure.

2.1.4 Additional Steps Required When Installing Patches Before Cluster Creation

This note applies only if you install a patch kit before creating a cluster; that is, if you do the following:

1. Install the Tru64 UNIX base kit.
2. Install the TruCluster Server kit.
3. Install the Version 5.1B patch kit before running the `clu_create` command.

In this situation, you must then perform three additional steps:

1. Run `versw`, the version switch command, to set the new version identifier:

   # **/usr/sbin/versw -setnew**

2. Run `versw` to switch to the new version:

   # **/usr/sbin/versw -switch**

3. Run the `clu_create` command to create your cluster:

   # **/usr/sbin/clu_create**

2.1.5 When Taking a Cluster Member to Single-User Mode, First Halt the Member

To take a cluster member from multiuser mode to single-user mode, first halt the member and then boot it to single-user mode. For example:

```
# shutdown -h now
>>> boot -fl s
```

Halting and booting the system ensures that it provides the minimal set of services to the cluster and that the running cluster has a minimal reliance on the member running in single-user mode.

When the system reaches single-user mode, run the following commands:

```
# /sbin/init s
# /sbin/bcheckrc
# /usr/sbin/lmf reset
```

2.1.6 Problems with clu_upgrade switch Stage

If the `clu_upgrade switch` stage does not complete successfully, you may see a message like the following:

```
versw: No switch due to inconsistent versions
```

The problem can be due to one or more members running `genvmunix`, a generic kernel.

Use the command `clu_get_info -full` and note each member's version number, as reported in the line beginning

```
Member base O/S version
```

If a member has a version number different from that of the other members, shut down the member and reboot it from `vmunix`, the custom kernel. If multiple members have the different version numbers, reboot them one at a time from `vmunix`.

2.2 Summary of TruCluster Software Patches

This section provides brief descriptions of the patches in Patch Kit 1 for the TruCluster Server software products.

Number: Patch 2.00

Abstract: Fix for aliasd daemon

State: New

Modifies the aliasd daemon to include interface aliases when determining whether or not an interface is appropriate for use as the ARP address for a cluster alias when selecting the proxy ARP master.

Number: Patch 5.00

Abstract: Fix for initialization of Memory Channel driver

State: New

This patch:

- Fixes a regression for single physical rail Memory Channel configurations, and cleans up stale data left on an offline physical rail by the Memory Channel driver.
- Fixes issues associated with the initialization of the Memory Channel driver.

Number: Patch 7.00

Abstract: Fixes an issue with ICS on NUMA-based systems

State: New

This patch fixes an issue with ICS (Internode Communication Services) on a NUMA-based system in a cluster.

Number: Patch 14.00

Abstract: Cluster specific fix for mounting cluster root domain

State: New

This patch enables a cluster to boot even if the cluster root domain devices are private to different cluster members. Although this is not a recommended configuration, it should not result in an unbootable cluster. Currently, this is with respect to cluster root domains not under LSM control.

Number: Patch 17.00

Abstract: Fixes memory leak in cluster alias subsystem

State: Supersedes Patch 15.00

This patch:

- Fixes a problem in which cluster alias connections are not distributed among cluster members according to the defined selection weight.
- Fixes a memory leak in the cluster alias subsystem.

Number: Patch 19.00

Abstract: Fix for Oracle startup failure

State: New

This patch fixes a problem in one of the shipped rc scripts whereby Oracle fails during startup on a clustered system.

Number: Patch 22.00

Abstract: Fixes panic seen on LAN cluster running under load

State: Supersedes Patch 20.00

This patch:

- Corrects a problem involving discarded UDP datagrams that do not come from the correct port.
- Corrects a problem in which a panic displaying the message “error CNX MGR: cnx_comm_error: invalid node state” occurs on a LAN cluster running under load when other members are rebooting.

Number: Patch 26.00

Abstract: Problems with LSM disks and cluster quorum tool

State: New

This patch corrects problems with LSM disks and the cluster quorum tools. When a member having LSM disks local to it is down, the quorum tools fail to update quorum. This causes other cluster commands to fail.

Number: Patch 33.00

Abstract: Fix for CAA daemon

State: New

This patch:

- Addresses an error "caa_register -u" produces with no balance data.
- Corrects a problem with resource inaccessibility if the hosting member crashes during a remote caa_stop operation.

Number: Patch 35.00

Abstract: Fix for cluster alias manager SUITlet

State: New

This patch fixes a problem that causes the cluster alias manager SUITlet to falsely interpret any cluster alias with virtual={t|f} configured as a virtual alias regardless of its actual setting.

Number: Patch 37.00

Abstract: Security (SSRT2265)

State: New

This patch corrects a potential security vulnerability which, under certain circumstances, could compromise system integrity.

Number: Patch 39.00

Abstract: Reliable DataGram kernel thread problem

State: New

This patch fixes a problem in which an RDG (Reliable DataGram) kernel thread can starve other timeshare threads on a uniprocessor cluster member. In particular, system services such as networking threads can be affected.

Number: Patch 43.00

Abstract: Fixes a cluster member hang

State: Supersedes Patch 24.00

This patch:

- Addresses an assertion caused by a bad user pointer passed to the kernel via sys_call.
- Corrects a condition that causes a node to hang during testing the of Memory Channel cable pulls. A cluster member sometimes hangs when a Memory Channel cable is pulled, the node is taken down, the cable is plugged back in, and the node is rebooted.

Number: Patch 46.00

Abstract: Fixes a cluster deadlock

State: Supersedes Patches 8.00, 9.00, 10.00, 12.00, 41.00, 44.00

This patch:

- Fixes a problem that causes a hang to occur when multiple nodes are shutting down simultaneously.
- Fixes a problem that causes a Cluster File System panic when using raw Asynchronous I/O.
- Adds code to assist in problem diagnosis.
- Relieves pressure on the CMS global DLM lock by allowing AutoFS auto-UNmounts to back off.
- Updates the attributes on a directory when files are removed by a cluster node that is not the file system server.
- Fixes a problem of excessive FIDS_LOCK contention that occurs when large number of files are using system-based file locking.
- Fixes a cluster deadlock that may occur during failover and recovery when direct I/O is in use.
- Corrects diagnostic code that might result in a panic during kernel boot.
- Prevents a panic when an AutoFS file system is auto-unmounted.

Number: Patch 48.00

Abstract: Fixes a cfsd core dumping problem

State: New

This patch fixes a problem with a cfsd core dump that can occur shortly after startup if cfsd is enabled then, or if it enabled later, soon after that. The problem requires applying a dsfmgr patch.

Number: Patch 50.00

Abstract: Fixes a regression associated with non-SCSI storage

State: Supersedes Patch 27.00, 28.00, 29.00, 31.00

This patch:

- Fixes a regression associated with non SCSI storage.
- Improves the responsiveness of EINPROGRESS handling during the issuing of I/O barriers by removing a possible infinite loop scenario that could occur due to the deletion of a storage device.
- Fixes a problem that causes a panic with the message "CNX MGR: Invalid configuration for cluster seq disk" during simultaneous booting of cluster nodes.
- Fixes a possible race condition between a SCSI reservation conflict and an I/O drain, which could result in a hang.
- Alleviates a condition in which a cluster member takes an extremely long time to boot when using LSM.
- Fixes a problem in the cluster kernel where a cluster member panics while doing remote I/O over the interconnect.
- Corrects an issue to allow the Device Request Dispatcher, DRD, to retry to get disk attributes when EINPROGRESS is returned from the disk driver.
- Fixes a problem in which access to the quorum disk can be lost if the quorum disk is on a parallel SCSI bus and multiple bus resets are encountered.