Tru64 UNIX

Release Notes for Version 5.1B-3

Part Number: AA-RVGEC-TE

June 2005

Product Version: Tru64 UNIX Version 5.1B-3

This manual provides information on new and changed features for the HP Tru64 UNIX operating system. It also provides information on restrictions to the software and documentation.

The *Patch Summary and Release Notes* document that is included with Version 5.1B-3 in HTML and PDF formats provides additional information about this release, including a list of the changes it makes to the operating system, TruCluster Server software, and the Internationalization subset. You can access the *Patch Summary and Release Notes* on the CD or from the directory on which you install Version 5.1B-3.

The *Technical Update for Version 5.1B or higher* describes issues that were discovered after new 5.1B versions have been released. You can access that document from the following URL:

http://h30097.www3.hp.com/docs/updates/V51B/TITLE.HTM

Hewlett-Packard Company
Palo Alto, California

Contents

4 New and Changed Features in Versions 5.1B-2 and 5.1B-1

Index

About This Manual

This manual describes significant new and changed features in the HP Tru64 UNIX Version 5.1B-3 operating system software, as well as features that were introduced in Versions 5.1B-1 and Version 5.1B-2. It also provides release notes for Version 5.1B-3, including issues you should be aware of when installing and running Version 5.1B-3.

Audience

These release notes are for the person who installs the product and for anyone using the product following installation.

Organization

This manual is organized as follows:

Chapter 1	Contains an overview of new and changed features in Version 5.1B-3 of the operating system software.
Chapter 2	Describes issues to be aware of when installing or removing Version 5.1B-3.
Chapter 3	Contains information on issues pertaining to the operating system and TruCluster Server software.
Chapter 4	Contains information on new and changed features that were introduced in Version 5.1B-1 and Version 5.1B-2.

Related Documents

You will find it helpful to have the following documentation available during the installation of this product:

- The hardware documentation for your system
- The *Installation Guide*
- The *Installation Guide — Advanced Topics*
- The online reference pages
- The HTML files provided on the Software Documentation CD, especially *New and Changed Features from Previous Releases*

You can also view the *Technical Update* for Version 5.1B or higher for any additional information not included in these notes. You can access the *Technical Update* from the following Web site:

Reader's Comments

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

You can send your comments via Fax to the following number:

- 603-884-0120 Attn: UBPG Publications, ZKO3-3/Y32

Please include the following information along with your comments:

- The full title of the manual.
- 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 HP technical support office. Information provided with the software media explains how to send problem reports to HP.

Conventions

The following conventions are used in this manual:

%	
$	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells.
#	A number sign represents the superuser prompt.
% **cat**	Boldface type in interactive examples indicates typed user input.
file	Italic (slanted) type indicates variable values, placeholders, and function argument names.
[|]	
{ | }	In syntax definitions, brackets indicate items that are optional and braces indicate items that are

	required. Vertical bars separating items inside brackets or braces indicate that you choose one item from among those listed.
...	In syntax definitions, a horizontal ellipsis indicates that the preceding item can be repeated one or more times.
`cat`(1)	A cross-reference to a reference page includes the appropriate section number in parentheses. For example, `cat`(1) indicates that you can find information on the `cat` command in Section 1 of the reference pages.
Ctrl/*x*	This symbol indicates that you hold down the first named key while pressing the key or mouse button that follows the slash. In examples, this key combination is enclosed in a box (for example, Ctrl/C).

1

Version 5.1B-3 Overview

This chapter describes the new and changed features provided in the Version 5.1B-3 release of the Tru64 UNIX operating system and TruCluster Server software. It also describes enhancements to the `dupatch` utility used to install and maintain the Version 5.1B-3 release.

Note

The consolidated patch kit, which contains both functional enhancements and fixes, has been renamed Version 5.1B-3 CD-ROM. Formerly this kit would have been referred to as Version 5.1B-3/PK5 CD-ROM.

You need a valid software license to use HP Tru64 UNIX Version 5.1B-3 in order to be entitled to use the code on the Version 5.1B-3 CD-ROM. A valid software license to use HP Tru64 UNIX Version 5.1B-3 can be purchased separately or through the ownership of a valid software update license, which can be purchased separately or via an update support agreement which includes license to use, license subscription, or rights to use new versions of software.

1.1 Operating System Improvements

The Tru64 UNIX Version 5.1B-3 combines several resiliency code enhancements along with the latest patch kit onto one physical media called the Version 5.1B-3 CD-ROM. The Version 5.1B-3 kit has undergone full product qualification testing as a single entity on multiple configurations and is binary compatible with all previous Version 5 stream releases.

The following sections discuss new functionality for Tru64 UNIX Version 5.1B-3.

1.1.1 AdvFS robustness

The Advanced File System (AdvFS) code base received several resiliency enhancements that primarily involve making the code more robust.

1.1.2 Collect Support for Dynamic Changes to AdvFS Volumes

The `collect` utility has been enhanced to support dynamic changes to AdvFS volumes, such as the mounting and unmounting of filesets. A number of resiliency enhancements and improved error logging were also added to this utility.

1.1.3 Storage Handling Improvements

The Tru64 UNIX storage subsystem will now conduct a more robust search to determine if an alternate SAN path to a target SCSI disk exists prior to giving up on the I/O. The search will check for other paths or try to get a specific error code.

Traditionally when an I/O fails, the system retries a fixed number of times and then stops trying. With SCSI storage, in most cases the problem is a target failure; that is, the disk is no longer present or it has an unrecoverable error, as is the case with old or failing devices.

In some instances, however, a SAN might have a dead switch unit that is taking commands but not returning anything. In these cases, the operating system will now check for alternate paths and try to obtain a specific error code before giving up on the I/O.

Additional support was also added to enable faster failover for the Logical Storage Manager (LSM). See Section 1.3 for details.

1.1.4 Accounting

Refinements to the accounting of end-user utilization time on Tru64 UNIX accounting enables finer granularity in the measurement of how many resources an individual end user consumes over the complete duration of a session, even if it extends beyond 24 hours.

1.1.5 New Variables Provide Protection Against Attack

Two new kernel tunable variables, `tcp_rst_win` and `tcp_syn_win`, protect systems against two potential vulnerabilities called TCP RST attack and TCP SYN attack. For more information, see Section 3.1.1 and the revised `sys_attrs_inet`(8) reference page, which is installed with this kit.

1.1.6 New /etc/printcap Option

A new boolean `/etc/printcap` option, `sr`, suppresses the reprinting of jobs under conditions that indicate to the print daemon that a reprint is needed. The syntax for this entry is similar to that of the `sh` (suppress header) option.

You can use this option to suppress an unexpected or unneeded reprinting of jobs that are completed but are reprinted a second time due to miscommunication between the printer and the print daemon.

Note that if you set this option, even incomplete jobs that trigger reprint conditions will not be reprinted.

In addition, there is a fix to remote job reprinting in this patch kit that can trigger reprints which, under conditions previously described, do not appear to be needed.

1.2 TruCluster Server Improvements

he following list describes the TruCluster Server improvements for Tru64 UNIX Version 5.1B-3:

- Faster cluster boot time

  Large TruCluster Server configurations may experience quicker booting as a result of the increased scalability added to the kernel group services (KGS).

  KGS previously had a pre-allocated number of threads, and once that threshold was reached the only way to free up additional threads was to reboot the cluster. Threads will now be allocated dynamically as needed, thus enable shorter boot times for large cluster configurations.

- Clusterwide `fuser` command

  A new option, `-a`, has been added to the `fuser` command to expand the scope of a query to search for all users on cluster members. The current usage of the `fuser` command that returns information on users active on a specific cluster node remains unaltered.

  See the `fuser`(8) reference page installed with this kit for additional information.

- Cluster application availability

  Past behavior of the Cluster Application Availability (CAA) daemon dictated that report generation could take between 20 to 30 minutes to process. With this release, a resiliency enhancement resulted in a considerable reduction in the amount of time it took to generate a similar report. With this improvement, a report that would have taken 25 minutes to run can now be generated in about 5 minutes.

- Cluster alias serviceability enhancements

- Improved LSM performance within a clustered environment.

  See Section 1.3 for details.

1.3 LSM Enhancements

This release includes the following improvements to the Logical Storage Manager (LSM) for Tru64 UNIX Version 5.1B-3:

- Fastfail variable for mirrored volume I/O

  A new LSM tunable attribute for mirrored volume I/O, `lsm_fastfail_enable`, limits retries on some device errors.

  When set to `1`, this new `sysconfigtab` variable will improve application response time for some device errors, allowing LSM to detach a plex faster, using another mirror to service the I/O request.. The variable is off by default (`lsm_fastfail_enable=0`).

  Costly delays can occur on some device errors as retries are being serviced. Consider older I/O storage subsystems, for example, where devices are growing more error-prone. Although the retries may eventually result in successful I/O completion, there is no guarantee that will happen.

  The `lsm_fastfail_enable` variable causes potentially faulty plexes to detach faster, thereby allowing I/O to continue faster via a serviceable plex. With this policy set, plex detaches may not be an indication of a bad disk, but possibly an intermittent problem that slows I/O. Therefore, this policy is off by default, because plex detaches may occur more frequently. As with any plex detach, administrator action will be required to restore redundancy.

  The fastfail policy is targeted for those environments that have strict application response time requirements and active administration.

  If fastfail is enabled and the CAM layer of the I/O subsystem does not retry a request to an underlying disk of a LSM mirrored volume, the following entry will be logged in the binary error log for that request:

  ```
  Fastfail requested, not retrying
  ```

  If fastfail is enabled and LSM cannot find a mirror to satisfy the I/O request, it will retry the request with fastfail disabled for that request. A message will be logged to `/var/adm/messages` as an LSM volio message; for example, “lsm: volio: read error on volume mirvol1, retry with 'fastfail' off.” Both the binary error log and messages file detail can be examined through the evmlogs as well.

  Note that fastfail does not apply to mirrored volumes in recovery.

  For LSM sysconfig details, see the `sys_attrs_lsm`(5) reference page that is installed with this kit.

- LSM startup and disk rescans

  LSM performance enhancements can improve LSM startup and disk rescan operations.

1.4 Changes to Reference Pages

The following Tru64 UNIX reference pages have been revised for Version 5.1B-3 and are delivered in this kit:

btcreate(8)	clua_services(4)	collect(8)
csh(1)	disklabel(8)	dump(8)
envconfig(8)	freezefs(8)	fuser(8)
ifconfig(8)	ip6rtrd(8)	ip6rtrd.conf(4)
kdbx(8)	mt(1)	netstat(1)
nifftmt(7)	ntp.conf(4)	psradm(8)
restore(8)	sh(1b)	sys_attrs_clua(5)
sys_attrs_ee(5)	sys_attrs_inet(5)	sys_attrs_lsm(5)
sys_attrs_ipv6(5)	sys_attrs_vm(5)	sys_attrs_vfs(5)
wtmpfix(8)	xntpd(8)	

1.5 New and Updated Associated Products

Several software products provided on the Associated Products CD–ROMs have been updated for this release. The following sections describe the updated products.

1.5.1 Volume 1

The following products on the Volume 1 CD have been updated.

1.5.1.1 Advanced Server for Tru64 UNIX

The Advanced Server for Tru64 UNIX (ASU) software has been updated to Version 5.1B-3. This update provides enhancements and corrections for problems found in the ASU Version 5.1B-2 ECO1 software, and in earlier versions of the ASU software.

Enhancements and corrections in the ASU Version 5.1B-3 kit include the following:

- The ASU server is now able to notify clients of changes made by UNIX programs and commands.
- The ASU server now supports mailslot messages sent to the cluster alias IP address.

- ASU now supports locales with an expanding character set such as the UTF-8 codeset, for example, fi_FI.UTF.8 or ja_JP.UTF-8, for file names and pathnames.
- Interoperability between `smbfs` on a Linux client and the ASU server has been improved.
- The `elfread` command has been enhanced with three new options for managing ASU event log settings.
- A new registry parameter, `MemberUseAnyDC`, can improve connection response time by allowing an ASU member server to use any available domain controller for validating authentication requests.
- Two new `lanman.ini` parameters, `logunixpasswordchgsuccess` and `logunixpasswordchgfailure`, have been added under the `[lxserver]` section to control the logging of UNIX password changes by the `ASDUPASS` utility, and also by the ASU server when the `SyncUnixPassword` registry entry is enabled.
- The `pccheck` client toll has been enhanced with a new option, `-escalate`, to collect the system configuration of Windows NT systems. The files are collected in compressed form, as a cab file, in the `pccheck` directory.

1.5.1.2 binaryScan

The `binaryScan` utility for Tru64 UNIX has been updated to Version v2.1. This update includes reporting capabilities for TruCluster and AdvFS related APIs and an updated database. More information about `binaryScan` is available at the following Web site:

`http://devresource.hp.com/drc/resources/binaryScan/download.jsp`

1.5.1.3 DataDirect Drivers

DataDirect Connect for ODBC has been updated to Version 5.0. This is the fastest, most comprehensive suite of ODBC drivers for all major databases.

DataDirect SequeLink has been updated to Version 5.4. This highly scalable, server-based middleware gives you a complete platform for data connectivity.

1.5.1.4 hpuxman

The `hpuxman` utility has been updated to Version 1.1. This update includes the HP-UX 11i v2 reference pages. More information about `hpuxman` is available at the following Web site:

http://devresource.hp.com/drc/resources/Tru64_UNIX_to_HP-UX_hpuxman_v11.jsp

1.5.1.5 LDAP Utilities

The LDAP utilities product has been updated to include the latest OpenLDAP tools from version 2.2.15, minor fixes, and general improvements.

1.5.1.6 OpenLDAP Directory Server

OpenLDAP has been updated to version 2.2.15. This update includes fixes and general improvements.

1.5.1.7 Mozilla

Mozilla has been updated to version 1.7.5. This update includes fixes and some new features. For a description of the new features provided in this version, see the Mozilla release notes at the following Web site:

http://www.mozilla.org/releases/mozilla1.7.5/README.html

1.5.2 Volume 2

The following products on the Volume 2 CD have been updated.

1.5.2.1 Legato NetWorker

Legato NetWorker for HP Tru64 UNIX has been updated to Version 7.2, which includes the following new or enhanced features:

- Direct file access with advanced file type devices
- Increased device support limits for power edition
- Data service agent
- Firewall support enhancements
- NDMP index processing improvements
- NetWorker storage node support for NDMP clients

1.5.2.2 Motif

A buffer overflow on the `libXpm` library was corrected.

1.5.2.3 Secure Web Server

The Secure Web Server has been updated to Version 6.4.0 with this release. This update includes Apache-1.3.32, Apache-2.0.52, and Tomcat-5.0.28.

1.5.2.4 UniCensus Utility

The UniCensus utility has been updated to Version 5.0.6 with this release.

1.5.2.5 Web Based Enterprise Service

The Web Based Enterprise Service (WEBES) has been updated to Version 4.4.1 with this release. Features in this release include the following:

- Disaster Tolerant Consulting Services (DTCS) notification (via XML) of all callouts made by WEBES
- WEBES can now send an SNMP service trap notification to HP Systems Insight Manager (HP SIM) when a hardware or crash notification needs to be made.
- The `wsea test nosys` command was reinstated as in versions prior to Version 4.4

1.6 Changes to the dupatch Utility

Beginning with Version 5.1B-2, HP changed to the way Tru64 UNIX patch kits are installed by introducing the concept of Inclusive Patch Kits. If you did not install Version 5.1B-2 but have installed earlier kits, you may want to review an overview of the installation changes as described in the *Patch Kit Installation Instructions* and in Section 4.1.2.1.

Version 5.1B-3 introduces several new changes to the installation and patch removal process:

- Before you can install this kit you must accept the conditions included in the license that the `dupatch` utility displays. You can read this license in the *Patch Summary and Release Notes*, included on the Version 5.1B-3 CD-ROM.
- You can now delete the kit by kit name rather than by specifying individual patches. With the introduction of this feature, you can easily delete patches interactively using the `dupatch` utility or from the `dupatch` command line. This feature also works on pre-Version 5.1B-3 kits.
- You can delete patches in multiuser mode.
- You can force the installation of the patch kit even if file conflicts exist. This feature is an extension of the `dupatch` baselining feature.
- A new command-line option, Patch Level, provides a single command that provides a full description of the patch kits, CSPs, and ERPs installed on your system.

For complete details of these features and step-by-step instructions on using them, see the *Patch Kit Installation Instructions*.

2

Version 5.1B-3 Installation and Deinstallation Notes

This chapter describes issues to be aware of when installing or removing Version 5.1B-3. Section 2.2 describes general issues, while Section 2.3 describes issues specific to installing and removing Version 5.1B-3 on a cluster using the rolling upgrade procedure.

2.1 Choosing and Installing the Software You Need

The following sections provide brief overviews of the CD-ROMs included in this kit and point you to the information you need to install the software.

2.1.1 CD-ROM Overview

This kit contains six primary CD-ROMs. The following list describes the contents of those disks and tells you what you need to know to get your system up and running as quickly as possible:

- Version 5.1B-3 CD-ROM

  This disk contains the new and improved features and problem fixes described in this manual. If your system is already running Version 5.1B or higher, installing the software on this disk will bring your operating system to Version 5.1B-3.

  This disk will also update the TruCluster Server software and internationalization subset to Version 5.1B-3 if those products are installed on your system.

- Tru64 UNIX Version 5.1B Operating System CD-ROM

  This disk contains the Tru64 UNIX Version 5.1B operating system. You will need to install the software on this disk if one of the following conditions exists:

  - Your operating system is not already running Tru64 UNIX Version 5.1B or higher
  - You are installing Tru64 UNIX on a new system

- Associated Products Volumes 1 and 2 CD-ROMs

  These disks contain software products that run on the Tru64 UNIX operating system. The *Read This First* letter included with this kit lists

the products on these CDs and Section 1.5 describes which products have been updated for this release. Install the products that you want to access on your system or any of the updated products for which you want to run the latest versions.

Note that TruCluster Server software included on Volume 2 is Version 5.1B. If your system is already running the TruCluster software and you want to add the new features and problem fixes included in Version 5.1B-3, install the software included on the Version 5.1B-3 CD-ROM.

- Tru64 UNIX Version 5.1B documentation CD-ROM

  This disk contains the manuals that provide information for general users, system administrators, and programmers using the Tru64 UNIX system. If the Version 5.1B documentation set is already installed, do not install the software on this CD.

  Note that the Version 5.1B-3 CD-ROM installs all reference pages that have been updated since the Version 5.1B release, if the reference page subset is installed on your system. Section 1.4 lists the reference pages that have been revised for Version 5.1B-3. The *Patch Summary and Release Notes* manual included on the Version 5.1B-3 CD-ROM lists the reference pages that have been revised in previous Version 5.1B updates.

- New Hardware Delivery-7

  This disk enables support for new hardware. The release notes for this or prior NHD-7 releases describes the new hardware that NHD-7 supports. If you are not installing Version 5.1B on one of the platforms listed in the release notes or have not added any of the hardware listed, do not install the software on this disk.

  Note that if you do install the NHD-7 software (if, for example, you are installing Tru64 UNIX on a DS15), this disk will automatically install the Version 5.1B-3 update.

2.1.2 Installing the Software

The procedure you use to install the components of your kit depends on the current state of your system. The following list can get you started with the most common installation procedures:

- New, update, or preinstalled operating systems

  If this is a new or update installation, or an installation that was preinstalled (called factory installed systems, or FIS), begin by reviewing the Tru64 UNIX *Installation Instructions* guide. See Section 1.2 for FIS systems and Section 1.3 to determine the type of installation that best meets your needs.

  To access the *Installation Instructions*, install the Tru64 UNIX Documentation Library as described in the Version 5.1B-3 *Read This*

First letter. The *Installation Instructions* manual is included with the documentation set's System and Network Management Documentation library.

- Installing on a cluster

  If you are installing on a cluster, start with Section 1.4 of the *Installation Instructions* for guidance in obtaining the information you need.

- Installing associated products

  Appendix D of the Tru64 UNIX *Installation Instructions* will guide you through the process of installing one or more of the Associated Products provided on the two Associated Products disks included with the Version 5.1B-3 kit.

- Updating to Version 5.1B-3

  If you are updating your Version 5.1B system to Version 5.1B-3 and do not need to install the features provided on the New Hardware Delivery 7 CD-ROM, see the CD mounting instructions included in the *Read This First* letter included with your Version 5.1B-3 kit. Those instructions also point you to the *Patch Kit Installation Instructions* that will guide you through the process, including installing Version 5.1B-3 on a cluster.

- Installing the New Hardware Delivery-7 kit

  If you are installing the NHD-7 kit included with Version 5.1B-3, you do not have to separately install Version 5.1B-3 — that kit will be installed as part of the NHD-7 installation procedure.

  See the section on NHD-7 in the *Read This First* letter. Then follow the CD mounting instructions in that letter as described for the Version 5.1B-3 CD. After mounting the CD, you can access the NHD-7 *Release Notes and Installation Instructions*.

2.2 Operating System Notes

The release notes in the following sections provide important information about the Version 5.1B-3 installation and deinstallation process, as well as general information about the operating system.

2.2.1 Possible Error Seen During Version 5.1B-3 Installation

You may see the following messages when installing Version 5.1B-3.

```
1200600:/sbin/hwmgr: /sbin/loader: Error:
         libpthread.so: symbol "_callback_rmutex" unresolved
1200600:/sbin/hwmgr: /sbin/loader: Fatal Error:
        Load of "/sbin/hwmgr" failed: Unresolved symbol name
```

These messages are generated as a result of the order in which components are installed and can safely be ignored.

2.2.2 Possible Errors Seen After Version 5.1B-3 Installation

The following problems have been known to occur after Version 5.1B-3 has been installed:

- The Common Data Security Architecture (CDSA), IP Security Protocol (IPsec), or Single Sign-On (SSO) do not work.
- The following error message is displayed during boot time:

```
CSSM_ModuleLoad: CSSM error 4107
```

If you experience these problems, make sure that the following command line has been executed:

```
# /usr/sbin/cdsa/mod_install -f -i -s \
/usr/lib/cdsa/libt64csp.so -d /usr/lib/cdsa/
```

2.2.3 Message Seen During Reboot Can Be Ignored

The following error message will be displayed after you reboot your system the first time after installing Version 5.1B-3:

```
AllowCshrcSourcingWithSubsystems is not valid
ForcePTTYAllocation is not valid
IdentityFile is not valid
AuthorizationFile is not valid
```

These messages are caused by a new version of SSH included in Version 5.1B-3. They do not pose a problem and can be ignored.

2.2.4 Enabling the Version Switch After Installation

Some of the software installed with Version 5.1B-3 requires you to run the `versw -switch` command to enable the new functions delivered in those patches. (See the *Patch Kit Installation Instructions* for information about version switches.) Enter the following command after `dupatch` has completed the installation process:

```
# versw -switch
```

The new functionality will not be available until after you reboot your system. You do not have to run the `versw -switch` command, but if you do not, your system will not be able to access the functionality provided in the version-switch patches.

2.2.5 Special Instruction File May Be Overwritten

When installing multiple products using the `dupatch` command, the file that causes Special Instructions to be displayed (`/var/adm/patch/doc/Special_Instructions.txt`) may be overwritten.

To ensure that you have access to all available special instructions, enter the following commands:

```
# cd /var/adm/patch/doc
# cat *.special_instruction
```

2.2.6 Required Actions When Uninstalling Version 5.1B-3

The following sections describe actions you have to take if you decided to uninstall Version 5.1B-3. Read each section before running the patch deletion procedure.

2.2.6.1 Script Required to Reverse Version Switch

If you enabled the version switches as described in Section 2.2.4, you must run the `/usr/sbin/versw_enable_delete` script before attempting to remove Version 5.1B-3. The steps for running this script require a complete cluster or single system shutdown, so choose a time when a shutdown will have the least impact on your operations. The following steps describe the procedure:

1. Make sure that all phases of the installation process have been completed.
2. Run the `/usr/sbin/versw_enable_delete` script:

   ```
   # /usr/sbin/versw_enable_delete
   ```
3. Shut down the entire cluster or the single system.
4. Reboot the entire cluster or the single system.
5. Run `dupatch` on your single system or on a cluster using the rolling upgrade procedure to delete Version 5.1B-3 (as described in the *Patch Kit Installation Instructions*), up to the point where the kernel is rebuilt and the system must be booted.
6. Reboot the single system or each member of the cluster.

Note

This step requires that you reboot each cluster member to remove Version 5.1B-3. Because the no-roll procedure automatically reboots the system after deleting the patches, you would not be able to perform this step as required.

2.2.6.2 Changes to System May Need to Be Reversed

If you made the following changes to your system after installing this patch kit, you will have to undo those changes before you can uninstall it:

- If you changed your hardware configuration (for example, by adding a new disk), the system configuration that existed prior to installing

this patch kit might not recognize the new devices or may not provide the necessary support for them.

- If you added new cluster members, the new members will not have an older state to revert to if you attempt to uninstall this patch kit.

To uninstall this kit, do the following:

1. Remove all new hardware and new cluster members that you added after installing this kit.
2. Run `dupatch` to uninstall the patch kit.
3. Verify that the patch kit was successfully uninstalled.

You can now add the cluster members you removed and reinstall the hardware you removed, as long as the support for it existed in the pre-patched system. You can also reinstall the patch kit.

2.2.6.3 Script Required when Returning to Pre-Patched System

If removing this patch kit restores your system to a pre-patched state, you must run the `/etc/dn_fix_dat.sh` script before rebooting your system during the patch-deletion process.

This situation would occur if Version 5.1B-3 is the only Tru64 UNIX patch kit installed on your 5.1B system.

Failing to run this script will result in your system being unable to boot normally. If this occurs, do the following:

1. Boot your system in single-user mode:

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

2. Run the script:

```
# /etc/dn_fix_dat.sh
```

3. Reboot normally.

If you also need to reverse the version switch as described in Section 2.2.6.1, run the `/etc/dn_fix_dat.sh` script after step 5 in that process.

Note

If during the `dupatch` installation and deletion processes you see a Special Instruction about running this script, ignore that instruction unless your system meets the requirements described here.

2.2.7 Additional Steps Required for HP Insight Management Agents Kit

Under certain conditions, you will be prevented from installing Version 5.1B-3 if you are running HP Insight Management Agents kit CPQIM310 or higher or had a version of the kit previously installed. Those conditions are as follows:

- Your system contains a pre-Version 5.1B-3 kit and the Insight Management Agents kit.

  In this case, upgrading to this kit gives the following error message:

  ```
  Patch 26020.00 - SP04 OSFCLINET540 (SSRT3653 SSRT2384 SSRT2275 ...)
  ./sbin/init.d/snmpd: its origin can not be identified.

  This patch will not be installed.
  ```

- Your system contains Patch Kit 2,Patch Kit 3, or Patch Kit 4 and the Insight Management Agents kit was once installed but has since been removed.

  In this case, upgrading to Version 5.1B-3 gives the following error message:

  ```
  Patch 26020.00 - SP04 OSFCLINET540 (SSRT3653 SSRT2384 SSRT2275...)
  ./etc/pmgrd_iorate.config:  does not exist on your system,
  however, it is in the inventory of installed subsets.

  This patch will not be installed.
  ```

To work around this problem you will need to run the `dupatch` baseline process before installing Version 5.1B-3. The following steps will guide you through the process:

1. Make a backup copy of the `/sbin/init.d/snmpd` script. For example:

   ```
   # cp /sbin/init.d/snmpd /tmp
   ```

   An alternative to backing up this file in which you manually modify it is provided following step 7.

2. Run the Version 5.1B-3 `dupatch` utility and select Option 5, `Patch Baseline Analysis/Adjustment`. See the *Patch Kit Installation Instructions* for detailed instructions.

3. After Phase 5 of the baseline procedure, answer `y` to the following question:

   ```
   Do you want to enable the installation of any of these patches? [y/n]: y
   ```

   Phase 5 reports patches that do not pass installation applicability tests due to the current state of your system. The installation of Patch 26020.00 was prevented because of changed system files. The `dupatch` utility reports the known information about the files contained in each patch and asks if you want to enable the installation. Answering yes,

enables dupatch to install patches that were prevented from being installed due to unknown files.

4. Install Version 5.1B-3.
5. After the system is running with Version 5.1B-3 installed, stop the snmpd and insightd daemons as follows:

```
# /sbin/init.d/snmpd stop
# /sbin/init.d/insightd stop
```

6. Replace the /sbin/init.d/snmpd script with the one you copied in step 1; for example:

```
# cp /tmp/snmpd /sbin/init.d/snmpd
```

7. Start the snmpd and insightd daemons as follows:

```
# /sbin/init.d/snmpd start
# /sbin/init.d/insightd start
```

If you did not back up the /sbin/init.d/snmpd file in step 1, you can modify it after you install Version 5.1B-3 (step 4) and stop the snmpd and insightd daemons (step 5) as follows (the XXX represents the revision, such as 310):

1. Edit the line that reads CPQMIBS=/usr/sbin/cpq_mibs as follows:

```
CPQMIBS=/var/opt/CPQIMXXX/bin/cpq_mibs
```

2. Edit the line that reads PMGRD=/usr/sbin/pmgrd as follows:

```
PMGRD=/var/opt/CPQIMXXX/bin/pmgrd
```

3. Edit the line that reads $PMGRD > /dev/console 2>&1 & as follows:

```
$PMGRD '$RCMGR get PMGRD_FLAGS'  > /dev/console 2>&1 &
```

When you install a newer version of the Insight Management kit, the paths to the cpq_mibs and pmgrd subagents are changed in the snmpd script. By installing Version 5.1B-3, which includes Patch 26020, the snmpd script is replaced by the original version provided in the base version of the Insight Management kit. Because the use of that snmpd script will cause problems when using Insight Manager, you must restore the script to the latest version. To do this, restore the backup version you created in step 1 of the workaround procedure, or modify the replacement script as described in this section.

2.2.8 Change to executable_data Attribute Requires Running Script

Before setting the tunable attribute executable_data to a non-zero value, you must run the following script:

```
# /usr/sbin/javaexecutedata
```

2.2.9 Required Action when Installing Extended System V Functionality and Tru64 UNIX Worldwide Language Support Subsets from the APCDs

To successfully install the Extended System V Functionality and the Tru64 UNIX Worldwide Language Support subsets on the same system. take one of the following actions:

- If you have already installed the Extended System V functionality subsets, uninstall the subsets and then delete the `iconvTable` directory as follows:

  ```
  # rmdir /usr/lib/nls/loc/iconvTable
  ```

- If you have not yet installed the System V subsets, perform the following steps in the order presented:

  1. Install the Tru64 UNIX Worldwide Language Support subsets.
  2. Install the Extended System V Functionality subsets.
  3. Copy the following files:

     ```
     # cp /usr/i18n/lib/nls/loc/iconvTable/* /usr/lib/nls/loc/iconvTable
     ```

2.3 TruCluster Server Notes

The following release notes provide important information about the TruCluster Server software.

2.3.1 No-Roll Procedure Cannot Be Used to Remove Version 5.1B-3

To remove this patch kit, you must run the `/etc/dn_fix_dat.sh` script after rebuilding the kernel and before rebooting each member. If the script is not executed before rebooting, the system will fail to boot.

Because the no-roll procedure automatically reboots the system after deleting the patches, you would not be able to run the script as required. Therefore, the no-roll procedure cannot be used to remove this patch kit.

The workaround is to use the rolling upgrade procedure to remove this kit.

2.3.2 Do Not Install Prior NHD Kits on a Patched System

Do not install the NHD–5 or NHD–6 kits on your TruCluster system if you have installed this patch kit or earlier patch kits. Doing so may cause an incorrect system configuration. The installation code for these new hardware delivery kits does not correctly preserve some cluster subset files.

2.3.3 Updates for Rolling Upgrade Procedures

The following sections provide information on rolling upgrade procedures.

2.3.3.1 Select Option to Check Tagged Files (new)

During the preinstall stage of a rolling upgrade, you have the option of checking tagged files. You should override the default setting and select the check tag option. The reason for selecting this option is described in Section 2.3.3.2.

2.3.3.2 Check for Tagged Files if Messages Are Displayed (revised)

When installing this patch kit during a rolling upgrade, you may see the following error and warning messages during the setup stage:

```
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.
```

If you see these messages during the setup stage, you should verify that the tagged files were properly created when you execute the preinstall stage.

In cases where the tagged files are not created, you can repeat the setup stage.

2.3.3.3 Noncritical Errors

During a rolling upgrade to install this patch kit , you may encounter the following noncritical situations:

- The tagged file for `ifaccess.conf` (`.Old..ifaccess.conf`) may disappear. This error will not cause any problems with the rolling upgrade procedure or the installation of the kit. A message would alert you to this condition if you use the `clu_upgrade undo` command. Running the `clu_upgrade -v check setup` at the start of the procedure will fix this error.
- When the worldwide language subset is installed, the file `wwinstall` will attempt to be tagged and will fail. This error will not affect the operational status of the cluster.

2.3.3.4 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.

2.3.3.5 Do Not Add or Delete OSF, TCR, IOS, or OSH Subsets During Roll

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.

2.3.3.6 Undo Stages in Correct Order

If you need to undo the install stage, because the lead member is in an unrecoverable state, be sure to undo the stages in the correct order.

During the install stage, `clu_upgrade` cannot tell whether the roll is going forward or backward. This ambiguity incorrectly allows the `clu_upgrade undo preinstall` stage to be run before `clu_upgrade undo install`. Refer to the *Patch Kit Installation Instructions* for additional information on undoing a rolling patch.

2.3.3.7 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 the *Patch Kit Installation Instructions* and the `installupdate`(8) and `clu_upgrade`(8) reference pages.

2.3.3.8 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.

2.3.3.9 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 following procedure, perform the roll stage last on the member where AutoFS runs.

When it is 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.

2.3.4 Error on Cluster Creation

When you attempt to create a cluster after having deleted patches, you may see the following error messages:

```
*** Error ***
This system has only Tru64 UNIX patches installed.
Please install the latest TruCluster Server patches on your system.
You  can obtain the most recent patch kit from:
http://www.support.compaq.com/patches/
*** Error ***
The system is not configured properly for cluster creation.
Please fix the previously reported problems, and then rerun the
```

```
'clu_create' command.
```

If you see these messages, enter the following command:

```
# ls -tlr /usr/.smdb./*PAT*.sts
```

If this command returns a file with `000000` in its name, you will have to run the `clu_create` command with the `-f` option to force the creation of your cluster. The problem is caused by the cluster software misinterpreting the existence of some patches and will be corrected in a future patch kit.

If the command does not return a file with `000000` in its name, you will need to contact HP support to determine the cause of the problem.

2.3.5 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, enter the following commands:

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

3

Software Notes for Version 5.1B-3

This chapter provides release notes that are specific to Version 5.1B-3 and the TruCluster Server software subset included with it. If you have not previously patched your Version 5.1B system, including upgrading to Versions 5.1B-1 and 5.1B-2, be sure to read the *Patch Summary and Release Notes* document included on the Tru64 UNIX CD, which provides additional release notes you should be aware of. See the *00-READ-ME-FIRST* file on the Version 5.1B-3 CD for information about accessing the *Patch Summary and Release Notes*.

3.1 Base Operating System Notes

The following notes pertain to the base operating system.

3.1.1 Potential Security Vulnerability Identified

The industry standard TCP specification, RFC 793, has a vulnerability in which an attacker can reset established TCP connections using the TCP RST (reset) or SYN (synchronize) flags.

These packets need to have source and destination IP addresses that match the established connection as well as the same source and destination TCP ports.

The fact that TCP sessions can be reset by sending suitable RST and SYN packets is a design feature of TCP. According to RFC 793, an RST or SYN attack is only possible when the source IP address and TCP port can be forged (also called spoofed). In that case, TCP sessions, (including Telnet, SSH, SFTP, and HTTP) may be disconnected without warning. TCP sessions that have been disconnected can be re-established.

Normally, a TCP SYN packet (request for a new connection) that arrives on a server using a matching IP address, port number, and matching sequence number for an existing connection causes a TCP RST packet to be returned to the client. An attacker can guess the proper sequence number, along with the port and IP addresses, to cause an existing connection to be terminated with a TCP RST.

When a client is rebooted without closing an old connection to the server, a subsequent attempt to connect to the server that matches the old connection

tuple and sequence number will require a TCP RST in order to purge the old (stale) connection.

HP has addressed these potential vulnerabilities, called TCP RST attack and TCP SYN attack, by providing two new kernel tunable variables, `tcp_rst_win` (TCP RST window) and `tcp_syn_win` (TCP SYN window).

These variables mitigate the TCP reset attack by reducing the window sizes in which a TCP RST/SYN packet will be accepted by the Tru64 UNIX system.

The attributes for these variables are described in a revised `sys_attrs_inet`(5) reference page, which is installed on your system with the Version 5.1B-3 patch kit.

After the patch kit is installed, you can adjust the variables using the `sysconfig` and `sysconfigdb` commands, as described in the following sections.

3.1.1.1 Adjusting the tcp_rst_win Variable

You can adjust the TCP RST window variable, `tcp_rst_win`, as follows:

```
# sysconfig -q inet tcp_rst_win
  inet:
  tcp_rst_win = -1

# sysconfig -r inet tcp_rst_win=2048
  tcp_rst_win: reconfigured

# sysconfig -q inet tcp_rst_win
   inet:
      tcp_rst_win = 2048

# sysconfig -q inet tcp_rst_win > /tmp/tcp_rst_win_merge

# sysconfigdb -m -f /tmp/tcp_rst_win_merge inet

# sysconfigdb -l inet
   inet:
      tcp_rst_win = 2048
```

3.1.1.2 Adjusting the tcp_syn_win Variable

You can adjust the TCP SYN window variable, `tcp_syn_win`, as follows:

```
# sysconfig -q inet tcp_syn_win
  inet:
  tcp_syn_win = -1

# sysconfig -r inet tcp_syn_win=2048
  tcp_syn_win: reconfigured

# sysconfig -q inet tcp_syn_win
   inet:
      tcp_syn_win = 2048

# sysconfig -q inet tcp_syn_win > /tmp/tcp_syn_win_merge
```

```
# sysconfigdb -m -f /tmp/tcp_syn_win_merge inet

# sysconfigdb -l inet
   inet:
      tcp_syn_win = 2048
```

3.1.2 Modification to Changer Driver May Affect Some Applications

As a side effect of resolving issues with multiple access to the changer, the changer driver now requires a short period of exclusive access to the changer device as part of opening the device. For applications that have several threads or processes accessing a single changer simultaneously, this can result in waits for access to the changer device in the process of an open call. That wait can be lengthy as some changer commands can have long response times.

In general this behavioral change will not affect the overall throughput to a changer device, as this wait would have occurred at the time of any I/O (for example, IOCTLS) to the changer.

If having the changer wait in this fashion presents a problem, the old behavior can be approximated by passing either the `O_NONBLOCK` or `O_NDELAY` flags at the open of the changer device. In that situation the first actual I/O (usually an IOCTL) may incur the wait as the open is partially delayed in that case.

3.1.3 Data Sorting of Audit Records May Be Required on Single CPU Systems

The `net_tcp_stray_packet`, `net_udp_stray_packet`, and `net_tcp_rejectd_conn` network events are handled by the audit subsystem differently from other auditable events. As a result, these events may be placed into the audit log out of order with respect to other events.

Previously, the sorting of audit data on single CPU systems was unnecessary. This changed, however, when the capability for auditing these network events was introduced. Now, to view these network events in order with respect to other events, you must sort the data on a single CPU system. To do this, use the `audit_tool -S` command.

3.1.4 new_wire_method Tunable Attribute Retired

The tunable attribute `new_wire_method` has been retired. After you install this kit, setting `new_wire_method` to either 0 or 1 will no longer affect your system.

3.1.5 Stopping Daemons May Speed Administration Performance

When using Advanced File System (AdvFS) administration commands, the `advfsd` and `smsd` daemons rescan filesets, domains, and volumes for system information. Depending on the number of filesets, domains, and volumes, you may experience a pause — sometimes quite long — between the commands. If you experience this performance degradation, you may want to stop `advfsd` (required for `dtadvfs`, the AdvFS graphical user interface) and `smsd` (required for SysMan Station) daemons before running multiple AdvFS administration commands.

To stop the daemons enter the following commands:

```
# /sbin/init.d/advfsd stop
# /sbin/init.d/smsd stop
```

To restart the daemons enter the following commands:

```
# /sbin/init.d/advfsd start
# /sbin/init.d/smsd start
```

3.1.6 sendmail Application Size/Length Limits Can Cause Problems

When upgrading older releases of `sendmail`, be aware that the 5.1B version of `sendmail` (V8.11.1) has MIME header/content marker size limits and message header length limits. These limits have been added to stop a Denial of Service (DoS) attack on the `sendmail` server. The values default to the following:

```
MIME Header Length Size = 2048 characters
MIME Content Marker Size = 1024 characters
```

The `MaxHeadersLength` value is the maximum message header length allowed and its size can be installation dependent (the value defaults to 8192 bytes).

Some legacy applications may be affected by this security addition if the application is sending mail messages with long lines of text and no new-line markers. These limitations may cause `sendmail` to insert a carriage return at these boundaries.

To revert back to the old `sendmail` behavior, do the following:

1. Verify that the `V2/Digital` header line is in the `/var/adm/sendmail/sendmail.cf` file. If the line is there, proceed to step 2. If it is not there, add it above the `# predefined` line. For example:

   ```
   # vi sendmail.cf

          .
          .
   ############################################################
   ```

```
V2/Digital

# predefined
```

2. Add the following lines to the /var/adm/sendmail/sendmail.cf file:

```
O MaxMimeHeaderLength=0/0
O MaxHeadersLength=-1/-1
```

3. Restart sendmail

3.1.7 SIA sialog Use Limitation Required

The Security Integration Architecture (SIA) sialog logging process is only intended for use in debugging SIA problems. It should not be enabled for extended periods of time. Doing so can cause login delays or other problems.

Use the audit subsystem to monitor authentications on the system, not the sialog process

To disable sialog debug logging, delete the /var/adm/sialog file. For more information, see the sialog(4) and sia_log(3) reference pages and the Tru64 UNIX *Security Programming* manual.

This information will be included in a revised sialog(4) reference page that will be delivered in a future Version 5.1B update. The reference page will also be updated to note that when used in a TruCluster Server cluster, the sialog file is a cluster-wide file.

3.1.8 Reboot May Resolve Problem with Smart Array Controller

If a problem with your Smart Array controller generates the following message, try rebooting your system:

```
Smart Array at ciss(1) not responding - disabled.
```

If the reboot does not re-enable the hardware, you will need to call your HP support representative to have the unit repaired.

3.1.9 Fix Available for Potential System Thread Hangs

The following potential problems were discovered too late to be corrected with this release:

- Threads can hang when when running the vfast or defragment commands on an AdvFS domain in a cluster.
- Threads can hang when an AdvFS clone is mounted and at least two threads perform memory mapping to the same file.

You can, however, prevent these potential problems by downloading and installing the following Early Release Patch (ERP) :

BU050520_EW01

This fix is available on the following Web site:

`http://h30097.www3.hp.com/unix/EarlyReleasePatch-download.html`

This ERP will be incorporated into the next release.

3.2 TruCluster Server Notes

The following notes pertain to systems running the TruCluster Server software subset.

3.2.1 Login Failure Possible with C2 Security Enabled

Login failures may occur as a result of a rolling upgrade on systems with Enhanced Security (C2) enabled. The failures may be exhibited in two ways:

- With the following error message:

```
Can’t rewrite protected password entry for user
```

- With the following set of error messages:

```
login: Ignoring log file: /var/tcb/files/dblogs/log.00001: magic number 0, not 8
login: log_get: read: I/O error
Can’t rewrite protected password entry for user
```

The problem may occur after the initial reboot of the lead cluster member or after the rolling upgrade is completed and the `clu_upgrade switch` procedure has been run. The following sections describe the steps you can take to prevent the problem or correct it after it occurs.

3.2.1.1 Preventing the Problem

You can prevent this problem by performing the following steps before beginning the rolling upgrade:

1. Disable the `prpasswdd` daemon from running on the cluster:

```
# rcmgr -c set PRPASSWDD_ARGS \
"‘rcmgr get PRPASSWDD_ARGS‘ -disable"
```

2. Stop the `prpasswdd` daemon on every node in the cluster:

```
# /sbin/init.d/prpasswd stop
```

3. Perform the rolling upgrade procedure through the `clu_upgrade switch` step and reboot all the cluster members.

4. Perform one of the following actions:

   - If PRPASSWDD_ARGS did not exist before this upgrade (that is, if `rcmgr get` PRPASSWDD_ARGS at this point shows only `-disable`), then delete PRPASSWDD_ARGS:

```
# rcmgr -c delete PRPASSWDD_ARGS
```

- If PRPASSWDD_ARGS existed before this upgrade, then reset PRPASSWDD_ARGS to the original string:

```
# rcmgr -c set PRPASSWDD_ARGS \
"`rcmgr get PRPASSWDD_ARGS | sed 's/ -disable//'`"
```

5. Check that PRPASSWDD_ARGS is now set to what you expect:

```
# rcmgr get PRPASSWDD_ARGS
```

6. Start the prpasswdd daemon on every node in the cluster:

```
# /sbin/init.d/prpasswd start
```

7. Complete the rolling upgrade.

3.2.1.2 Correcting the Problem

If you have already encountered the problem, perform the following steps to clear it:

1. Restart the prpasswdd daemon on every node in the cluster:

```
# /sbin/init.d/prpasswd restart
```

2. Reboot the lead cluster member.
3. Check to see if the problem has been resolved. If it has been resolved, you are finished. If you still see the problem, continue to step 4.
4. Try to force a change to the auth database by performing the following steps:

   a. Use edauth to add a harmless field to an account, the exact commands depend on your editor. For example, pick an account that does not have a vacation set and add u_vacation_end:

```
# edauth
s/:u_lock@:/u_vacation_end#0:u_lock@:/
w
q
```

   b. Check to see that the u_vacation_end#0 field was added to the account:

```
# edauth -g
```

   c. Use edauth to remove the u_vacation_end#0 field from the account.

   If the edauth commands fail, do not stop. Continue with the following instructions.

5. Check to see if the problem has been resolved. If it has been resolved, you are finished.

   If you still see the problem, observe the following warning and continue to step 6.

Warning

Continue with the following steps only if the following conditions are met:

- You encountered the described problem while doing a rolling upgrade of a cluster running Enhanced Security.
- You performed all previous steps.
- All user authentications (logins) still fail.

6. Disable logins on the cluster by creating the file `/etc/nologin`:

```
# touch /etc/nologin
```

7. Disable the `prpasswdd` daemon from running on the cluster:

```
# rcmgr -c set PRPASSWDD_ARGS \
"`rcmgr get PRPASSWDD_ARGS` -disable"
```

8. Stop the `prpasswdd` daemon on every node in the cluster:

```
# /sbin/init.d/prpasswd stop
```

9. Force a checkpoint of `db_checkpoint`, using the `db_checkpoint` command with the `-1` (number 1) option :

```
# /usr/tcb/bin/db_checkpoint -1 -h /var/tcb/files
```

   Continue with the instructions even if this command fails.

10. Delete the files in the `dblogs` directory:

```
# rm -f /var/tcb/files/dblogs/*
```

11. Force a change to the `auth` database, as follows:

    - Use the `edauth` command to add a harmless field to an account. The exact commands depend on your editor. For example, pick an account that does not have a vacation set and enter the following:

```
# edauth
s/:u_lock@:/u_vacation_end#0:u_lock@:/
w
q
```

    - Check to see that the `u_vacation_end#0` field was added to the account:

```
# edauth -g
```

    - Use the `edauth` command to remove the `u_vacation_end#0` field from the account.

Warning

If the edauth command fails, do not proceed further. Contact HP support.

12. If the edauth command was successful, perform one of the following actions:
    - If PRPASSWDD_ARGS did not exist before this upgrade (that is, if rcmgr get PRPASSWDD_ARGS at this point shows only -disable), then delete PRPASSWDD_ARGS:

      ```
      # rcmgr -c delete PRPASSWDD_ARGS
      ```

    - If PRPASSWDD_ARGS existed before this upgrade, then reset PRPASSWDD_ARGS to the original string:

      ```
      # rcmgr -c set PRPASSWDD_ARGS \
      "`rcmgr get PRPASSWDD_ARGS | sed 's/ -disable//'`"
      ```

13. Check that PRPASSWDD_ARGS is now set to what you expect:

    ```
    # rcmgr get PRPASSWDD_ARGS
    ```

14. Start the prpasswdd daemon on every node in the cluster:

    ```
    # /sbin/init.d/prpasswd start
    ```

15. Re-enable logins on the cluster by deleting the file /etc/nologin:

    ```
    # rm /etc/nologin
    ```

16. Check to see if the problem has been resolved. If it has not, contact HP support.

3.2.2 Increasing RDG max_objs Value Recommended

For certain applications where Oracle instances are running in a cluster and Memory Channel is used as the interconnect, console messages of "rdg: out of objects" may occur.

Tuning the sysconfigtab value max_objs (under the rdg subsystem) can eliminate these messages. We recommend doubling your current value.

Because this parameter is not dynamic, you can only change it by modifying the sysconfigtab file and rebooting your system. After doing this, observe your cluster to see if the messages have been eliminated.

You can set this value to a maximum of 50,000.

3.2.3 Filesystem Unmount Recommended if Message Is Displayed

Under certain error conditions, the following message may be seen during a relocation or failover, or during the boot of a member:

```
WARNING: Unable to failover /mnt: pfs and cfs fsids differ
```

The result is that the fileset in question is now unserved in the cluster. For example:

```
# cfsmgr /mnt

        Domain or filesystem name = /mnt
        Server Status : Not Served
```

If this occurs, HP recommends that you immediately do the following:

1. Enter the following command to unmount the filesystem:

   ```
   # cfsmgr -u -p [mountpoint]
   ```

2. If other mounted filesets exist in the same domain, unmount them (they should also be in the "Not Served" state):

   ```
   # cfsmgr -u -d [domain]
   ```

   For steps on checking an AdvFS domain, see the *AdvFS Administration Guide*, Section 6.3.1, steps 3-7.

3. Run diagnostics on the domain before remounting its filesystems.

   To verify the domain, you can use the AdvFS `verify` utility or the `fixfdmn` utility. If using `fixfdmn`, HP recommends first running it with the `-n` option to see what errors are found before allowing `fixfdmnn` to fix them.

Once you have successfully verified the domain, remounting the domain's file systems in the cluster should succeed.

If the domain cannot be immediately verified, HP recommends that you do not remount the original fileset until this can be done.

Note

In rare cases, the warning message will be accompanied by a system panic. This will occur if CFS error handling is unable to successfully unmount the underlying physical file system. If this occurs, the console will direct you to use `cfsmgr` to unmount the domain on one of the remaining nodes prior to rebooting the member.

This action will prevent the rebooted member from attempting to failover-mount the filesystem and will minimize access to the domain. Prior to remounting the filesystem, it is advisable that the domain be sanity-checked using the steps given above.

3.3 Processor Notes

The following notes pertain to processor issues.

3.3.1 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 the Tru64 UNIX Version 5.1B operating system and patch kit to be installed.

3.3.1.1 Time Loss on Systems with Firmware Lower Than V6.4-12

The ES47, ES80, and GS1280 AlphaServers may experience a time loss as a result of console callbacks for environmental information if the server's firmware is lower than V6.4-12.

Updating your firmware to V6.4-12 or higher will keep the problem from occurring or correct the problem if it has occurred.

If your firmware is lower than V6.4-12, the problem is experienced if one or both of the following conditions exists:

- The system manager uses the following `hwmgr` utility commands:

```
# hwmgr -view devices
# hwmgr -view hierarchy
```

- The Environmental Monitoring daemon, `envmond`, is running.

As a workaround to the problem, you can modify one of the following two files and then reboot your system for the new setting to take effect:

- `/etc/rc.config`

  Turn off environmental monitoring by changing the entry `ENVMON_CONFIGURED=1 to ENVMON_CONFIGURED=0`

  You can also use the `envconfig` utility to modify the `/etc/rc.config` file. See `envconfig`(8) for information.

- `/etc/sysconfigtab`

  At the end of the file, add the following line:

```
marvel_srvmgmt: MV_Env_Support = 0
```

  You must remove this setting after you install firmware V6.4-11 or higher.

3.3.1.2 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.

3.3.1.3 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 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.

3.3.1.4 Hardware SCSI Bus Errors

SCSI CAM errors experienced by the KZPEA 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.

3.3.1.5 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.

3.3.2 Potential False Temperature Error Condition on AlphaServer DS10, DS10L, and TS10 Systems

A sensor error can potentially indicate a false over-temperature condition on AlphaServer DS10, DS10L, and TS10 systems. While the sensor accurately reports the temperature, it falsely reports the high temperature threshold. This false reporting of the threshold value can cause the Insight Management SNMP Agents to forward false traps, and potentially result in the Tru64 UNIX environmental monitoring daemon (envmond(8)) initiating the shutdown process. However, this false reporting condition is temporary and the high temperature threshold soon returns to normal, at which point the shutdown is cancelled.

To work around this problem, use the envconfig utility to manually set the high temperature threshold to its current default value. While this does not change the value, the act of setting it manually forces envmond to use the manually applied value. Once manually set, the ENVMON_HIGH_THRESH variable persists in the /etc/rc.config database. This will permanently work around the issue for current and future envmond sessions. To manually set the variable, follow these steps:

1. Determine the value of ENVMON_HIGH_THRESH:

```
# sysconfig -q envmon | grep thresh
# env_high_temp_thresh = 60
```

2. Manually set the threshold value using the envconfig utility:

```
# envconfig -c ENVMON_HIGH_THRESH=60
```

3.4 Documentation Notes

The following notes pertain to Tru64 UNIX documentation issues.

3.4.1 AdvFS Administration Manual Correction — Extend an AdvFS File System when Increasing the Size of the Underlying Volume

In Section 2.3.4.3 of the *AdvFS Administration* manual — "Increasing Storage in Domains by Extending an Existing Volume" — a step is missing from the procedure when the underlying storage volume is a hardware RAID device. You must modify the volume's disk label information to reflect the new, increased size of the partition supporting the domain, and then apply the updated disk label to the volume before extending the file system.

The complete process to extend a domain by increasing the size of an underlying hardware RAID volume includes the following steps:

1. Using HSG80 commands, extend the hardware RAID volume.

This might involve adding another stripeset to an existing stripeset, or creating a concatset from the original hardware RAID volume and adding another volume to it.

For example, assume the AdvFS domain uses disk dsk25c, which is a single hardware RAID volume. To extend the capacity of the disk, create a concatset from it and another single hardware RAID volume, as shown in the following example:

```
HSG80> show disks [1]
Name          Type                      Port Targ  Lun        Used by
------------------------------------------------------------------------------

DISK10000     disk                         1    0    0        DELI-5.1A
DISK10100     disk                         1    1    0        SPARESET
DISK10200     disk                         1    2    0        D8          [2]
DISK20000     disk                         2    0    0        DELI-5.1A
DISK20100     disk                         2    1    0        SPARESET
DISK20200     disk                         2    2    0                    [3]
DISK30000     disk                         3    0    0        GALLO-M1
DISK30200     disk                         3    2    0
DISK40000     disk                         4    0    0        GALLO-M1
DISK40200     disk                         4    2    0
DISK50000     disk                         5    0    0        GALLO-M2
DISK50200     disk                         5    2    0
DISK60000     disk                         6    0    0        GALLO-M2
DISK60200     disk                         6    2    0
HSG80> add concatsets C1 DISK10200 [4]
HSG80> set C1 add=DISK20200 [5]
HSG80> show C1 [6]
Name          Storageset                  Uses             Used by
------------------------------------------------------------------------------

C1            concatset                   DISK10200        D8
                                          DISK20200
        State:
          NORMAL
          DISK10200 (member  0) is NORMAL
          DISK20200 (member  1) is NORMAL
        Size:             71112778 blocks [7]
```

The following list explains each step:

[1] Find unused disks — those with an empty (blank) Used by field.

[2] DISK10200 (also called D8) is used by the AdvFS domain that will be extended. This storage volume is recognized as dsk25 on Tru64 UNIX.

[3] DISK20200 is unused.

[4] Create a concatset called C1 from DISK10200.

[5] Add DISK20200 to concatset C1 to create a larger disk.

[6] Display the size of the concatset C1.

[7] Note the size, because you will need to modify the disk label for dsk25 on Tru64 UNIX to match it.

2. Return to the Tru64 UNIX prompt.
3. Save a copy of the old disk label information for the volume:

   # **disklabel -r dsk*N* > /tmp/*label***

   For example:

   # **disklabel -r dsk25 > /tmp/dsk25MOD**
4. Edit the saved label and increase the size of the partition used by AdvFS:

   # **vi /tmp/*label***

   For example:

   # **vi /tmp/dsk25MOD**
5. Write the edited disk label back to the hardware RAID volume:

   # **disklabel -R dsk*N* /tmp/*label***

   For example:

   # **disklabel -R dsk25 /tmp/dsk25MOD**
6. Optionally, display the size of the domain before extending it:

   # **showfdmn *domain***

   For example, for a domain called `clinical_trials`, enter:

   # **showfdmn clinical_trials**

```
             Id              Date Created  LogPgs  Version  Domain Name
3e8ca76d.040d38c8  Thu Apr  3 16:28:13 2003     512        4  clinical_trials

  Vol   512-Blks        Free  % Used  Cmode  Rblks  Wblks  Vol Name
   1L   35556384    35547280      0%     on    256    256  /dev/disk/dsk25c
```

7. Extend the AdvFS file system:

   # **mount -u -o extend */file_system***

   For example, if the AdvFS domain that uses `dsk25` is mounted on `/test_data`, enter:

   # **mount -u -o extend /test_data**
8. Optionally, verify that the domain now shows the larger size:

   # **showfdmn *domain***

   For example:

   # **showfdmn clinical_trials**

```
             Id              Date Created  LogPgs  Version  Domain Name
3e8ca76d.040d38c8  Thu Apr  3 16:28:13 2003     512        4  clinical_trials

  Vol   512-Blks        Free  % Used  Cmode  Rblks  Wblks  Vol Name
   1L   71112768    71103120      0%     on    256    256  /dev/disk/dsk25c
```

3.4.2 Installation Guide Contains Incorrect Java Version

The *Installation Guide* states that Version 1.3.1-1 of Java is provided with Version 5.1B of the operating system. This is incorrect. Java Version 1.3.1-2 is provided with the Version 5.1B release of the operating system.

Version 5.1B-3 of the operating system includes Java Version 1.4.1-2.

3.4.3 System Configuration and Tuning Guide Corrections

Section 4.2 of the *System Configuration and Tuning* guide provides an example demonstrating how to enable access to the system's real time clock. This example is incorrect. The correct command is:

```
# mknod /dev/timedev c 15 0
```

Section 4.4.8.4 states: "The `max_async_req` attribute specifies the maximum number of sessions within any given RDG context table. The recommended value is at least the number of Oracle® processes plus two." This is incorrect. The `max_sessions` attribute specifies the maximum number of sessions within any given RDG context table.

Section 4.4.8.5 states: "The `max_async_req` attribute specifies the maximum number of pages automatically wired in memory for message packets." This is incorrect. The `rdg_max_auto_msg_wires` attribute specifies the maximum number of pages automatically wired in memory for message packets. HP recommends setting this attribute to 0.

Section 6.2.2.2 states that, if you increase the value of the `max_proc_per_user` attribute, you increase the amount of wired memory. This statement is false. Increasing this attribute value does not increase the amount of wired memory.

3.4.4 ypset(8) Correction

The `ypset`(8) reference page indicates that both V1 and V2 are allowed as options. This is incorrect. V2 is not a supported option.

3.4.5 aio_return(3) Correction

The following information should be appended to the RETURN VALUES section of `aio_return`(3):

On an unsuccessful call, the value of -1 is returned and `errno` is set to indicate the error. If the operation did not complete, but it terminated normally (because, for example, the call was purposely interrupted by the `aio_cancel` function), `errno` is set to 0.

3.4.6 disklabel(8) Correction

The following definition of the output from the `disklabel` command is missing from recent versions of `disklabel`(8):

An asterisk (*) is sometimes shown in the output from the `disklabel` command, under the column headed cylinders grouped for a partition (`cpg`).

This asterisk indicates that the start or the end of a cylinder does not fall exactly on a block boundary.

3.4.7 dxshutdown(8) Correction

Since the release of Tru64 UNIX Version 5.0, the command `/usr/bin/X11/dxshutdown` is a wrapper shell script that runs the SysMan shutdown program. Prior to Version 5.0, `dxshutdown` was an X motif application. The X Motif version of `dxshutdown` is shipped in an obsolete subset. The new `dxshutdown` shell script can run the old version when it is installed as `/usr/bin/X11/dxshutdown_old`. Use the following command:

```
# /usr/bin/X11/dxshutdown -old
```

The current OPTIONS section of `dxshutdown`(8) is no longer applicable because suitlets use Tk and Tk uses X, not Xt. The only useful argument is `-focus` *hostname* when running on a cluster.

The SysMan application is no longer called Shutdown Manager. If invoked from the SysMan menu, the leaf is labelled "Shutdown the system" and the application is labelled "Shutdown targeted on *hostname*".

In the EXAMPLES section, the `/usr/dt/appconfig/help/C/DXshutdown.sdl` help file is no longer used. In the FILES section, `/usr/dt/appconfig/help/C/Dxshutdown.sdl` and `$HOME/Dxshutdown` are no longer used.

3.4.8 emx(7) Correction

The `emx`(7) reference page provides an example of how to turn off I/O limiting by using the following run-time configuration command:

```
# /sbin/sysconfig -r io NPort_Max_IOs = 0xFFFFFFFF
```

This example command should read as follows:

```
# /sbin/sysconfig -r emx NPort_Max_IOs=0xFFFFFFFF
```

3.4.9 dd(1) Correction

Note 1 in `dd`(1) provides an example of zeroing a disk label. The syntax of the `disklabel` command used in that example is incorrect and should read as follows:

```
# disklabel -r /dev/rdisk/dsk1a
# disklabel -z  /dev/rdisk/dsk1a
# disklabel: Disk /dev/rdisk/dsk1a is unlabeled
```

3.4.10 ksh(1) correction

In ksh(1), the following statements are incorrect:

- && Causes the list following it to be executed only if the preceding pipeline returns a 0 (zero) exit value.
- || Causes the list following it to be executed only if the preceding pipeline returns a nonzero exit value.

The correct statements are:

- && Causes the list following it to be executed only if the preceding pipeline returns a nonzero exit value.
- || Causes the list following it to be executed only if the preceding pipeline returns a 0 (zero) exit value.

4

New and Changed Features in Versions 5.1B-2 and 5.1B-1

The following sections describe new and changes features that were introduced in Versions 5.1B-2 and 5.1B-1. The information in these sections was previously published in the Versions 5.1B-2 and 5.1B-1 *Release Notes* documents.

4.1 New and Changed Features for Tru64 UNIX Version 5.1B-2

This section describes new features that are available with the Version 5.1B-2 release of the operating system. It also lists new hardware that is supported.

4.1.1 New Hardware Support

The following new hardware support has been added in this release:

- This release provides support for the upgraded EV7 Alpha chip operating at 1.3 GHz.
- HP StorageWorks DAT 40x6 Tape Autoloader: The HP StorageWorks DAT 40x6 tape autoloader is a dependable, entry-level solution for small-to-medium server storage and enterprise network backup needs.
- HP StorageWorks DLT VS80: The StorageWorks DLT VS80 tape drive provides affordable 80-GB backup to IT managers with midrange servers.
- FCA2684 and FCA2684DC: This adapter is a PCI-X 2GB 64-bit/133MHz single and dual port Fibre Channel Host Bus Adapter.

4.1.2 New Functionality

The following section discusses new functionality for Tru64 UNIX Version 5.1B-2.

4.1.2.1 Inclusive Patch Kits

The 5.1B-2/PK4 patch kit marked a new way of delivering Tru64 UNIX patches. If you installed previous Tru64 UNIX patch kits, you will see the following differences when you install this kit:

- All or none installation

  When you install an inclusive patch kit, you must install all patches; you can no longer select specific patches to install. By making the installation of all patches mandatory, you can patch with greater confidence that the process will be problem-free.

  Before a patch kit is released, it is tested on many types of systems and system configurations. This testing continues until we are sure that the patches perform the tasks they were designed for and do not introduce new problems. It is not possible to achieve this type of testing on every possible combination of individually selected patches.

- Substantially reduced installation time

  The installation process for inclusive patch kits can reduce the time it takes to install the patches by as much as half from what you are used to. For large, clustered systems, the difference can be several hours faster.

- Fewer patches displayed

  Because of the way these new patch kits are designed, you will see fewer patches listed by `dupatch` during the installation process. For example, a partial listing you see will be similar to the following:

```
- Tru64_UNIX_V5.1B / Security Related Patches:
      * Patch 25001.00 - SP04 OSFACCT540

      * Patch 25002.00 - SP04 OSFADVFS540 (SSRT2275)

      * Patch 25003.00 - SP04 OSFADVFSBIN540
```

  In the old-style patch kits, these three patches might have consisted of perhaps 20 individual patches being displayed. The difference is not in the content of the kits, but rather in the way the patches are packaged and installed. In this example, the `SP04` identifies the patch as belonging to Version 5.1B-2, the `OSF...540` identifies the subset the patch is included in, and the `SSRT2275` indicates a type of security patch.

  As with previous kits, you can find a brief overview of all the patches (listed by patch number) in the kit's *Patch Summary and Release Notes*.

- All or none patch removal

  As with the installation process, if you want to remove a patch, you must remove all of them. That is, you can no longer select individual patches for removal.

- Patches for Worldwide Language Support (WLS) subset

  Beginning with Version 5.1B-2, patch kits will include any patches that may be required for the WLS subset. As with the TruCluster Server patches, the WLS patches will only be installed if you have the WLS subset installed.

Except for the installation and removal processes, the functions provided by the `dupatch` utility generally work the same with inclusive patch kits as they do in old-style patch kits. For example, the Patch Tracking and Baselining menus remain the same and work the same in Version 5.1B-2 as they do in the old-style patch kits.

The *Patch Kit Installation Instructions* manual provides information for installing inclusive patch kits and the old-style kits. Where the processes differ, each process is explained.

4.1.2.2 Unified Buffer Cache Scaling

This release introduces Unified Buffer Cache Scaling, which improves large SMP and NUMA system performance. MSI interrupts entails implementing the PCI-X specification to allow the device to use >1 MSI. With EV7 and EV7z being PCI-X systems with MSI-capable devices and drivers, they are sure to see better performance from reduced locks, especially in large configurations.

4.1.3 TruCluster Server Improvements

The following sections describe TruCluster Server improvements for Tru64 UNIX Version 5.1B-2/PK4.

4.1.3.1 Faster Boot Times for TruCluster Server Environments Using LSM

This release contains enhancements that provide a significant reduction in the time required to boot TruCluster Server configurations using Logical Storage Manager (LSM).

4.1.3.2 Improved Memory Channel Performance During Peak System Utilization

The Memory Channel subsystem has been enhanced to support parallel Memory Channel input processing. This enhancement increases the Memory Channel performance, and provides resistance to CPU starvation.

4.1.3.3 Additional TruCluster Enhancements

The following additional TruCluster Server enhancements are new for this release:

- Sticky Cluster Connections: This is an attribute for a cluster alias that will direct all client connections to the same cluster node, providing a stickiness of a servicing cluster member to a specific client/port.
- Improved Cluster Serviceability: Improves the troubleshooting efficiency by providing a mechanism to retrieve runtime information from the cluster alias daemon (`aliasd`).

- Improved Cluster Manageability: TruCluster Server now supports the `sysconfig` command across the entire clusters, in much the same way that it currently runs on a single system.

  In a TruCluster Server environment, the `sysconfig` command uses the cluster interconnect to send requests to reconfigure, query attributes, and query subsystem states of kernel subsystems on different cluster members. The `sysconfig` command receives output from these commands across the cluster interconnect. Using the cluster interconnect for these commands allows querying or modification attributes on members that are hung or on members that do not have an external interface between cluster members.

  The cluster interconnect is not used for the `sysconfig configure` and `unconfigure` commands.

4.1.4 Networking Improvements

The following sections discuss the networking improvements for Tru64 UNIX Version 5.1B-2.

4.1.4.1 Mobile IPv6 Update

This release provides an update to the current Mobile IPv6 code to bring it in line with the latest Networking RFCs.

4.1.4.2 IPv6 Advanced API Update

The IPv6 advanced API has been updated to conform to RFC 3542.

4.1.4.3 pfilt_loopback and pfilt_physaddr

Two packetfilter tunable variables, `pfilt_loopback` and `pfilt_physaddr`, were previously tunable only by using `dbx`. These variables are now tunable using `sysconfig` and `/etc/sysconfigtab`. See Section 4.2.4 for more information about these variables.

4.1.5 Worldwide Language Support Improvements

The following sections describe the Worldwide Language Support improvements for Tru64 UNIX Version 5.1B-2.

4.1.5.1 Updated Localized Messages

Localized messages have been updated to match English messages that have changed since the release of Tru64 UNIX Version 5.1B.

4.1.5.2 Improved Asian TTY Subsystem

The Asian TTY subsystem has been improved to reduce the risk of kernel crashes under heavy workloads.

4.1.5.3 Enhanced Chinese Support

The Qu-Wei input method invoked from `dxhanziim` or `dxim` now produces a correct character from a Unicode value.

Characters are now drawn with the correct width in the zh_CN.GB18030 locale.

4.1.5.4 Improved Iconv Converters

Iconv converters for Japanese mainframe codesets (ibmkanji/JEF/KEIS) have been improved to reduce the number of incorrect results.

4.1.6 New and Updated Associated Products

Several software products provided on the Associated Products CD–ROMs have been updated for this release. The updated products are listed in the following sections.

4.1.6.1 Advanced Server for Tru64 UNIX

The Advanced Server for Tru64 UNIX (ASU) software has been updated to Version 5.1B-2. This update provides enhancements and corrections for problems found in the ASU Version 5.1B ECO2 software, and in earlier versions of the ASU software.

Some of the enhancements and corrections in the ASU Version 5.1B-2 kit:

- The ASU server can now be a Backup Domain Controller to a Windows 2003 mixed mode domain.
- The ASU server now supports the nondefault cluster alias. The ASU server supports only one cluster alias at a time, which can be either the default alias or a nondefault alias.
- The `FileChangeNotify` registry parameter has been added to enable the ASU server to notify clients of a file change from other clients.
- The `StoreAttributesAsMetadata` registry parameter has been added to enable storing of DOS attributes and file creation time in AdvFS metadata. This allows the use of DOS attributes irrespective of the `UseUnixGroups` registry parameter value, and preserves the file creation time when modifying a file. The default value is 0 (do not store DOS attributes and file creation time in AdvFS metadata).

- Three new ASU commands `chattr`, `lsattr`, and `rmattr`, are added to manage DOS attributes. See the associated reference pages for a description of each command.
- A new command, `prcheck`, is available to check and enumerate ASU printer entries, which includes the ASU printer share entries, printer printcap entries, printer registry entries, and printer spool directory entries.
- A new client tool, `pccheck`, is available to collect and display the diagnostic information such as user, share, network statistics, browse list, and connectivity to PDC/BDC.

4.1.6.2 Tru64 UNIX to HP-UX Software Transition Kit

The Tru64 UNIX to HP-UX Software Transition Kit has been updated to Version 2.2. The Tru64 UNIX to HP-UX Software Transition Kit has been updated to include a broader coverage of commands, libraries and programming languages. Tru64 UNIX developers can now use the STK to scan Fortran source code files in addition to C and C++, makefiles and shell scripts.

4.1.6.3 XEmacs

XEmacs has been updated to Version 21.1.14 with this release.

4.1.6.4 Secure Web Server

The Secure Web Server has been updated to Version 6.3.0 with this release.

4.1.6.5 Perl

Perl has been updated to Version 5.8.4 with this release.

4.1.6.6 Extended System V Functionality

The Extended System V Functionality has been updated to Version 2.1. This update includes new and modified commands and APIs, and updated reference pages.

4.1.6.7 UniCensus

UniCensus has been upgraded to Version 5.0.5 with this release.

4.1.6.8 Visual Threads

Visual Threads has been updated to Version 2.4–003 with this release.

4.1.6.9 Web Based Enterprise Service

The Web Based Enterprise Service (WEBES) has been updated to Version 4.3.3 with this release.

4.1.6.10 Collect GUI

The Collect GUI has been updated to Collgui ver 3.0 (build 13) with this release.

4.1.6.11 OpenLDAP Utilities

LDAP Utilities product is updated to include the latest OpenLDAP tools from version 2.1.25, minor bug fixes, and general improvements.

4.1.6.12 OpenLDAP Directory Server

The OpenLDAP Directory Server has been updated to version 2.1.25. This update includes bug fixes and general improvements.

4.1.6.13 Mozilla

Mozilla has been upgraded to Version 1.6. For a description of the new features provided in this version, see the Release Notes at the following URL:

http://www.mozilla.org/releases/mozilla1.6/README.html#new

4.1.6.14 Legato NetWorker

Legato NetWorker for HP Tru64 UNIX has been updated to Version 7.1. This update includes a number of new and advanced features.

4.2 New and Changed Features for Tru64 UNIX Version 5.1B-1

This section describes new features that are available with the Version 5.1B-1 release of the operating system. It also lists new hardware that is supported and provides information about retiring products.

4.2.1 Support for Tuning Big Pages Attributes of Binary Files

This release provides support for tuning binary files to have different big page behavior than system defaults. These settings can override the system defaults for specific types of memory (anonymous, program text, SysV shared, SysV shared segmented, and stack).

Each of the specific type settings has systemwide tunables, expressed as a threshold in kilobytes. The default is 64 KB, the size of the smallest big page. The per-binary tunables are also expressed as a threshold in kilobytes.

An additional tunable directs big pages to distribute memory across RADs as a priority over getting the largest page size possible.

For information about using this feature, see `chatr`(1) and `sys_attrs_vm`(5) and the *System Configuration and Tuning* guide.

4.2.2 Support for the Name Services Switch

The Name Service Switch (NSS) has been added to Tru64 UNIX as a replacement for the `svc.conf` database service selection. The NSS provides a more extensible database service selector and supports a dynamic list of databases. Using the NSS allows you to add LDAP as a source for `netgroup` data.

Configuring the NSS converts entries from the `/etc/svc.conf` file into entries for the `/etc/nsswitch.conf` file. The`/etc/svc.conf` is then only used for pre-`nsswitch` statically-built applications and Sendmail. For more information about this feature, see `nssetup`(8), `nsswitch`(4), and `nss2svc`(8).

4.2.3 New Security Feature

A new security feature prevents the execution of instructions that reside in heap or other data areas of process memory. The result is additional protection against buffer overflow exploits. This feature is similar in concept to Tru64 UNIX executable stack protection.

This feature is implemented as a dynamic `sysconfig` tunable attribute, `executable_data`, in the `proc` subsystem. The supported settings allow system administrators to cause requests from privileged processes for writable and executable memory to fail, or to be treated as a request for writable memory, and optionally to generate a message when such a request occurs.

In a buffer overflow exploitation, an attacker feeds a privileged program an unexpectedly large volume of carefully constructed data through inputs such as command-line arguments and environment variables. If the program is not coded defensively, the attacker can overwrite areas of memory adjacent to the buffer.

Depending upon the location of the buffer (stack, heap, data area), the attacker can deceive these programs into executing malicious code that takes advantage of the program's privileges or alter a security-sensitive program variable to redirect program flow.

With some expertise, such an attack can be used to gain root access to the system.

Enabling the executable_data tunable changes a potential system compromise into, at worst, a denial-of-service attack. A vulnerable program may still contain a buffer overflow, but an exploit that writes an instruction stream into the buffer and attempts to transfer control to those instructions will fail, because memory protection will prohibit instruction execution from that area of memory.

Many applications never execute from the memory even though they unnecessarily request write-execute memory directly or as a result of an underlying function acting on their behalf. By substituting writable memory for the requested write-execute memory, the executable_data tunable allows such applications to benefit from the additional protection without requiring application modification. See sys_attrs_proc(5) for more information.

Before enabling executable_data (changing it from the default value of 0), you must run the /usr/sbin/javaexecutedata script. Otherwise, privileged Java™ applications will fail in unpredictable ways. See javaexecutedata(8) for more information.

Note

The Java language interprets bytecode at run time. Unless marked as exempt, privileged applications written in Java will receive an error when they attempt to execute instructions residing in the unexecutable memory. The manner in which these errors are handled is application-specific and thus unpredictable. This is why you must run the /usr/sbin/javaexecutedata script before you enable executable_data.

The following example demonstrates the failing behavior to expect for a privileged processes if execute_data is set to 53 but runs the /usr/sbin/javaexecutedata script. Other Java applications run with privilege may exhibit different (but still failing) behavior.

```
# java -classic -jar SwingSet2.jar
Process 1185 Invalid write/execute mmap call denied.
Process 1185 Invalid write/execute mmap call denied.
Process 1185 Invalid write/execute mmap call denied.
(...)
Process 1185 Invalid write/execute mmap call denied.
Process 1185 Invalid write/execute mmap call denied.
**Out of memory, exiting**
```

The following example demonstrates the failing behavior to expect for a privileged processes if execute_data is set to 37 but runs the

/usr/sbin/javaexecutedata script. Other Java applications run with privilege may exhibit different (but still failing) behavior.

```
# java -classic -jar SwingSet2.jar
Process 1185 Invalid write/execute mmap call modified.
Process 1185 Invalid write/execute mmap call modified.
 (...)
Process 1185 Invalid write/execute mmap call modified.
Process 1185 Invalid write/execute mmap call modified.
Process 1185 Invalid write/execute mmap call modified.
SIGSEGV   11*  segmentation violation
(...)
Abort (core dumped)
```

Certain privileged Pascal programs may also fail when executable_data is enabled. Such programs should also be marked as exempt, using the new chatr utility, included in Patch 872.00 and described as follows:

```
$chatr +ed enable priv_pascal_executable
  current values:
     64-bit COFF executable
     execute from data: disabled
  new values:
     64-bit COFF executable
     execute from data: enabled
```

See chatr(1) for more information.

4.2.4 Packetfilter Enhancements

Enhancements were made to the following dbx kernel flags to control packetfilter-written packets:

- pfilt_loopback=[0|1] Setting this flag to 0 prevents a loop back of any packetfilter-written multicast or broadcast packet. When set to 1, the packetfilter loops back both broadcast and multicast packets. This is the default.
- pfilt_physaddr=[0|1] Setting this flag to 0 allows the application to fill in the source Ethernet address for packetfilter-written packets. If the source address is all 0s, the address is set to the proper hardware address by the packetfilter code as a safety precaution. When set to 1, the packetfilter sets the Ethernet source address in the outgoing packet. This is the default.

You can set these variables at boot time as follows:

```
# echo " patch pfilt_loopback=0 " | dbx -k /vmunix
# echo " patch pfilt_hysaddr=0 " | dbx -k /vmunix
```

Restriction

The pfilt_loopback and pfilt_physaddr tunable variables are only accessible in the kernel using dbx. In a future patch kit, these tunable variables will be implemented as kernel subsystem

configurable attributes, accessible through the `sysconfig` command.

4.2.5 New Hardware Support

The following new hardware support was added:

- Support for AlphaServer GS1280 systems configured with 64 processors.

  Support for AlphaServer and AlphaStation DS15 systems, including the following:

  - Alpha 1-GHz CPU with 2-MB onboard ECC cache
  - 512-MB, 1-GB, or 2-GB SDRAM memory - expandable to 4-GB
  - Onboard dual 10/100 BaseT Ethernet ports
  - Four 64-bit PCI expansion slots
  - Onboard Ultra160 SCSI controller
- Support has been added for the FCA2384 — 2 GB, 64-Bit/133 MHz PCI-X-to-Fibre Channel Host Bus Adapter.

4.2.6 New and Updated Associated Products

A number of software products provided on the Associated Products CD–ROMs have been updated for this release. The updated products are listed in the following sections.

For more information on the CD-ROM contents, see the *HP Tru64 UNIX Version 5.1B-1 CD-ROMs* card contained in the media kit.

4.2.6.1 Advanced Printing Software Version 1.2A

Advanced Printing Software has been updated to support the following printers:

Genicom mL210 PS
Genicom mL280 PS
Genicom LN21 PS
Genicom LN28 PS
Genicom cL160 PS
HP LaserJet 2300 Series Printers PS
HP LaserJet 4200 Series Printers PS
HP LaserJet 4300 Series Printers PS
HP LaserJet 5100 Series Printers PS
HP LaserJet 2500 Series Color Printers PS
HP LaserJet 4550 Series Color Printers PS

HP LaserJet 4600 Series Color Printers PS
HP LaserJet 5500 Series Color Printers PS

The list of supported printers can be found at the following URL:

http://h30097.www3.hp.com/printing/printers.html

4.2.6.2 Advanced Server for Tru64 UNIX

Advanced Server for Tru64 UNIX (ASU) has been updated to Version 5.1B ECO1. This update includes support for the following new features:

- The ASU server supports systems configured with LAG (Link aggregation) network support. You can configure the ASU server to listen on NetBIOS over TCP/IP and NetBEUI over the LAG interface.
- The ability to enable and disable event logging by the Event Manager (EVM).
- When negotiating a protocol with a remote server, the ASU server now sends the list of dialects that it supports in one SMB packet. This improves ASU server performance and keeps the lmx.dmn process from hanging when the remote server is Windows® NT®.

For a complete description of the changes made to ASU, read the release notes available at the following Web site:
http://h30097.www3.hp.com/docs/asdu/HTML/asdu.html

4.2.6.3 Application Transition Tools

The following Tru64 UNIX to HP-UX application transition tools have been added to the Associated Products CD-ROM:

- Tru64 UNIX to HP-UX Software Transition Kit Version 2.0 – This kit includes file scanning utilities, developer's documentation, and porting documentation to help resolve compatibility issues between Tru64 UNIX and HP-UX. The file-scanning utilities use a clear methodology for code analysis, providing sound advice for each Application Programming Interface (API) encountered in scanned Tru64 UNIX C and C++ source code files.
- appscan Version 2.0 – This utility enables you to list all of the dependencies (shared libraries and symbols) of a dynamic executable file. The utility also generates an associated disposition code for each of the listed APIs.
- hpuxman v1.0 – This command allows you to display select HP-UX 11i v1.6 reference pages on systems running the Tru64 UNIX operating system.

4.2.6.4 Compaq COBOL RTL

The Compaq COBOL RTL has been updated from Version 2.7 to Version 2.8-670.

4.2.6.5 OpenLDAP Directory Server

This is an update of the OpenLDAP Directory Server from Version 2.0.23 to Version 2.0.27. This update consists mainly of bug fixes and includes new versions of all of the OpenSource components.

4.2.6.6 OpenLDAP Utilities

The LDAP Client Utilities have been updated to Version 1.1. This update includes support for an additional configuration parameter, `nisnetgrpbranch`, added for LDAP netgroups support.

4.2.6.7 Mozilla Version 1.4 Application Suite for Tru64 UNIX

The Mozilla Application Suite is the next generation Web, mail, and news application successor to the popular Netscape Communicator Web client. Mozilla is an open source Web application created by the Mozilla Foundation. It is designed for standards compliance, performance, and portability.

The Mozilla 1.4 Application Suite also includes many new innovative features for search, privacy, and content management of your Internet information. Built upon the Netscape Gecko browser engine, the Navigator component is now comprehensive, modular, and fully standards compliant — supporting DOM, RDF, XML, CSS, and HTML 4 document formats.

4.2.6.8 Java

Java has been updated from Version 1.3.1 to Version 1.4.1–2.

4.2.6.9 Secure Web Server

Secure Web Server has been updated to Version 6.1. This update contains a new subset based on Apache 2 in addition to the older Version 1.3 code base. The update includes new versions of all of the OpenSource components.

4.2.6.10 Legato NetWorker

Legato NetWorker for HP Tru64 UNIX has been updated to Version 7.0. This update includes a number of new and advanced features.

4.2.6.11 WEBES

The Web Based Enterprise Service Suite has been updated to Version 4.2.

4.2.6.12 UniCensus

The UniCensus Revision and Configuration Management (RCM) application has been updated from Version 4.5.2 to Version 4.5.4.

4.2.6.13 Visual Threads

Visual Threads Version 2.3 offers the following new features:

- Enhancements to profiling and dynamic resizing of the Event Details window
- Fixes for the Summary and Print windows
- Fixes for deadlock and inconsistent Order detection

4.2.7 Sources for Open Source Components

In this release, a new CD–ROM has been added to the Tru64 UNIX media kit. This CD–ROM contains sources for Open Source Software provided with the Tru64 UNIX operating system.

The *Sources for Open Source Components* CD–ROM contains sources for the following products:

- Secure Web Server:

  Secure Web Server Administration Utility
  Secure Web Server Documentation
  Tomcat Java Servlet and JSP Engine
  Secure Web Server 1.3 powered by Apache 1.3
  Secure Web Server 2.0 powered by Apache 2.0

- LDAP Components

  OpenLDAP Directory Server
  LDAP Client Utilities

- Mozilla 1.4 for Tru64 UNIX

  Mozilla 1.4 Application Suite
  Mozilla 1.4 Runtime Support

4.2.8 Retirement Notices

This section provides information on features that have been retired from the operating system.

4.2.8.1 Aurema ARMTech Products Retirement

Aurema ARMTech products, ShareExpress, ShareExtra, and ShareEnterprise will be removed from the Tru64 UNIX operating system distribution before December 2003. HP will continue to be support ShareExpress through June 2004.

Aurema announced end of sales of the ShareExtra and ShareEnterprise products for Tru64 UNIX in June 2003. Aurema continues to directly support current customers.

4.2.8.2 DEC Ada Retirement

Section 2.2.8 of the Version 5.1B *Release Notes* incorrectly states that DEC Ada (UPI - 0HM) and DEC Ada PDO (UPI - 0VS) will be retired in a future release of the operating system.

DEC Ada was retired in March 2000.

Index

X