Contents

Tables............................................................................................................. vii

Preface........................................................................................................... ix

Who Should Read This Document.......................................................... ix
What This Document Contains............................................................... ix
What is New in this Revision................................................................. x
Publications.............................................................................................. xi
  Tivoli Policy Director for Operating Systems Library.............................. xi
  Prerequisite Publications...................................................................... xi
  Accessing Publications Online........................................................ xi
  Ordering Publications......................................................................... xi
  Providing Feedback about Publications............................................. xii
Contacting Customer Support.............................................................. xii
Conventions Used in This Book............................................................. xii
  Typeface Conventions........................................................................ xi

Chapter 1. About This Release.............................................................. 1

Chapter 2. Installation and Upgrade Notes........................................... 3
  Hardware Requirements for Installing Tivoli Policy Director for Operating Systems.............................................. 3
  Supported Operating System Levels and Required Patches...................... 4
  Software Provided with Tivoli Policy Director for Operating Systems............... 6
  Installation Notes................................................................................ 7
    Install Fails on HP-UX Systems with Patch PHCO_22526 Applied.................. 7
    Install of IBM SecureWay Directory Client Might Fail.............................. 8
    Patch Required for Tivoli Software Installation Service on Linux ................ 8
    Patch Required for Tivoli SecureWay Policy Director Connection Version 3.7 .................. 8
  Upgrade Notes...................................................................................... 8
    Changes to Initial Policy..................................................................... 8
    Policy Director Language Packs on Policy Director for Operating Systems NLS Support CD......................... 9
    Easy Install Procedure Revised to Include Silent Install.......................... 9
    Installing On All Platforms Using Easy Install.................................... 9

Chapter 3. Software Limitations, Problems, and Workarounds............. 13
  Space Errors on Heavily Loaded HP-UX Systems................................. 13
  AIX NIS Client and Tivoli Policy Director for Operating Systems Startup Order............................................ 13
  Policy Updates Occurring During Configuration Might Cause Errors........ 13
Notes Regarding Linux Systems ................................................... 26
  Configuration Change Needed on Some Internationalized Versions of Red Hat Linux 7.1 . . . . . 26
  Japanese Locale and Language Setting Supported on Linux Systems ............................... 26
  Tivoli Policy Director Considerations When Using International Locales on Linux Systems . . 26
Notes Regarding Solaris Systems ................................................... 27
  Setting the Locale for CDE Login on Solaris 2.8 ....................................................... 27
Tables

1. Memory Requirements .................................................................................. 3
2. Disk Space Requirements for Installation ................................................... 3
3. Supported Operating System Levels and Required Patches ....................... 4
4. Software Provided ......................................................................................... 6
Preface

The Tivoli Policy Director for Operating Systems Release Notes document provides an overview of the changes introduced in this release of Tivoli Policy Director for Operating Systems. This document also provides information that is either incorrect or missing from the product documentation as well as describes workarounds for any known problems encountered during the final testing of the product.

Information in this revised document supersedes information in the product documentation or in the product itself.

Note: IBM Tivoli Access Manager for Operating Systems is the new name of the software previously released as Tivoli Policy Director for Operating Systems. The product documentation for Version 3.8 was completed before the name change was decided upon. Since this document is part of that document set, the new name is not reflected in this version.

Who Should Read This Document

This document is intended for systems administrators who have some knowledge of these topics:

- UNIX® operating system
- Internet protocols, including HTTP, TCP/IP, FTP, TELNET, SSL
- Security management
- Directory services
- Authentication
- Authorization
- Tivoli Policy Director

Supplementary information that systems administrators may find useful includes knowledge of the following topics:

- Tivoli Management Environment framework
- Tivoli Distributed Monitoring
- Tivoli Enterprise Console®
- Tivoli Risk Manager
- Tivoli Security Manager
- Tivoli User Administration

What This Document Contains

The Tivoli Policy Director for Operating Systems Release Notes contains the following sections:

- Chapter 1, “About This Release” on page 1
  Introduces Tivoli Policy Director for Operating Systems and its functions.
- Chapter 2, “Installation and Upgrade Notes” on page 3
What This Document Contains

Describes the hardware and software prerequisites for installing Tivoli Policy Director for Operating Systems. Notes on installing or upgrading an existing installation also are provided.

- Chapter 3, “Software Limitations, Problems, and Workarounds” on page 13
  Describes any limitations or problems encountered in Tivoli Policy Director for Operating Systems during testing that could not be fixed in the final version of the product, along with any known workarounds.

- Chapter 4, “Documentation Notes” on page 23
  Describes any errors or omissions in the documentation provided with the product.

- Chapter 5, “Internationalization Notes” on page 25
  Describes any limitations or problems encountered in testing the internationalized versions of Tivoli Policy Director for Operating Systems that could not be fixed in the final version of the product, along with any known workarounds.

What is New in this Revision

This revision of the Tivoli Policy Director for Operating Systems Release Notes contains information that has been developed since the original document was completed or was omitted from the earlier version. Included in this document are the following topics:

- New operating systems supported
- Installation and upgrade information
- Policy Director Language Packs on Policy Director for Operating Systems NLS Support CD
- Easy Install Procedure Revised to include Silent Install
- PDOS Login Activity Policy on HP-UX 11x with rexec/remsh (replaces earlier release note entitled, "Locked User Can Still Use rexec on HP-UX 11.10")
- Execution of PDOS Tasks without root in osseal-admin
- Auth Requisite Modules on PAM Platforms
- Problems Unlocking the CDE Screen on AIX Systems after Installation/Configuration
- Considerations When Upgrading the Operating System on a Machine Running PDOS
- PDOS Login Activity Policy with $HOME/.rhosts and /etc/hosts.equiv
- Update to PDOSD Daemon not Autostarting on Japanese AIX systems
- Corrections to the Tivoli Policy Director for Operating Systems Installation Guide and Tivoli Policy Director for Operating Systems Administration Guide:
  - Some pdoscfg Options Incorrectly Documented
  - Additional Information on Task: Subscribe PDOS Endpoints
  - Information About Kill Permission is Incorrect
- Command-line Arguments Added to the se2pdos Utility
- Corrections to the original version of the Tivoli Policy Director for Operating Systems Release Notes
New topics are located at the end of their respective sections; revised topics were changed in place.

Publications

This section lists publications in the Tivoli Policy Director for Operating Systems library and any other related documents. It also describes how to access Tivoli publications online, how to order Tivoli publications, and how to make comments on Tivoli publications.

Tivoli Policy Director for Operating Systems Library

The following documents are available in the Tivoli Policy Director for Operating Systems library:

- **Tivoli Policy Director for Operating Systems Installation Guide**
  Provides information about installing Tivoli Policy Director for Operating Systems.

- **Tivoli Policy Director for Operating Systems Administration Guide**
  Provides information on using Tivoli Policy Director for Operating Systems and includes a reference of the commands available.

- **Tivoli Policy Director for Operating Systems Release Notes**
  Provides late-breaking information about Tivoli Policy Director for Operating Systems.

Prerequisite Publications

To be able to use the information in this guide effectively, you must have some prerequisite knowledge, which you can get from the following books:

- **Tivoli SecureWay® Policy Director Base Administration Guide, Version 3.8**
- **Tivoli SecureWay Policy Director Base Installation Guide, Version 3.8**
- **Tivoli SecureWay Policy Director Release Notes, Version 3.8**

Accessing Publications Online


These publications are available in PDF or HTML format, or both. Translated documents are also available for some products.

Ordering Publications

You can order many Tivoli publications online at the following Web site: [http://www.ibm.com/shop/publications/order](http://www.ibm.com/shop/publications/order)

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968
- In other countries, for a list of telephone numbers, see the following Web site: [http://www.tivoli.com/inside/store/lit_order.html](http://www.tivoli.com/inside/store/lit_order.html)
Providing Feedback about Publications

We are very interested in hearing about your experience with Tivoli products and documentation, and we welcome your suggestions for improvements. If you have comments or suggestions about our products and documentation, contact us in one of the following ways:

- Send an e-mail to pubs@tivoli.com.
- Complete our customer feedback survey at the following Web site: [http://www.tivoli.com/support/survey/](http://www.tivoli.com/support/survey/)

Contacting Customer Support

If you have a problem with any Tivoli product, you can contact Tivoli Customer Support. See the *Tivoli Customer Support Handbook* at the following Web site: [http://www.tivoli.com/support/handbook/](http://www.tivoli.com/support/handbook/)

The handbook provides information about how to contact Tivoli Customer Support, depending on the severity of your problem, and the following information:

- Registration and eligibility
- Telephone numbers and e-mail addresses, depending on the country you are in
- What information you should gather before contacting support

Conventions Used in This Book

This book uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface Conventions

The following typeface conventions are used in this book:

**Bold**

Lowercase and mixed-case commands, command options, and flags that appear within text appear like *this*, in **bold** type.

Graphical user interface elements (except for titles of windows and dialogs) and names of keys also appear like *this*, in **bold** type.

**Italic**

Variables, values you must provide, new terms, and words and phrases that are emphasized appear like *this*, in *italic* type.

**Monospace**

Commands, command options, and flags that appear on a separate line, code examples, output, and message text appear like *this*, in **monospace** type.

Names of files and directories, text strings you must type, when they appear within text, names of Java methods and classes, and HTML and XML tags also appear like *this*, in **monospace** type.
About This Release

This release of Tivoli Policy Director for Operating Systems includes the following features and enhancements:

**New Operating Systems Supported**
The following new operating system platforms are supported:
- AIX 5.1
- HP-UX 11.11 (11i)
- Red Hat Linux 6.2 (x86)
- Red Hat Linux 7.1 (x86)
- Red Hat Linux 7.2 (x86)
- SuSE Linux 7.3 (x86)

**Designating Non-Root Users as Runtime Administrators and Auditors**
Changes were made to the initial Tivoli Policy Director for Operating Systems policy that help establish more distinct roles for Tivoli Policy Director for Operating Systems runtime administrators and auditors. These changes also make it possible to establish non-root users as Tivoli Policy Director for Operating Systems runtime administrators and auditors and to remove the native root user from being a runtime administrator or auditor.

When installing Tivoli Policy Director for Operating Systems from the Tivoli desktop, there is a new option available that allows you to specify additional logins that are allowed to administer the Tivoli Policy Director for Operating Systems runtime.

A new task called Add/Remove PDOS Auditors/Administrators has been added to the PDOS Management Tasks. Users, including the root user, can be added or removed as Tivoli Policy Director for Operating Systems runtime administrators or auditors using this task. Adding and removing users as runtime administrators and auditors also can be achieved by directly managing the Tivoli Policy Director osseal-admin and osseal-auditors groups and the osseal and ossaudit UNIX groups.

**Tivoli Enterprise Console Support**
Events generated by Tivoli Policy Director for Operating Systems can now be sent to the Tivoli Enterprise Console.

**Tivoli Risk Manager Support**
Tivoli Policy Director for Operating Systems now integrates with Tivoli Risk Manager.
**Trusted Computing Base (TCB) Enhancements**

Files in the Trusted Computing Base (TCB) are checked on a periodic basis and on execution attempts for unexpected changes to the file’s signature. A file’s creation time, or *ctime*, is part of the file’s signature. If the ctime of the file changes, the file is marked untrusted in the TCB. Some backup utilities change a file’s ctime even when the file has not changed. This activity causes the file to get marked untrusted in the TCB unnecessarily. The `-tcb_ignore_ctime` option of the `pdoscfg` command has been added to alleviate this problem. When the `-tcb_ignore_ctime` option is enabled, ctime is ignored when performing file signature checks.

Checking a file’s signature also involves running a CRC check. For large binary files, avoiding the CRC check at execution time might be desirable. The `-tcb_nocrc_on_exec` option of the `pdoscfg` command has been added to allow you to bypass the CRC check. When this option is enabled, the PDOSD daemon skips the CRC check when checking a binary file’s signature prior to execution.

**Improved Login Activity Policy Integration in NIS Environments**

The `pdoslpadm` command has been enhanced to allow an administrator to configure a Network Information Service (NIS) server to support password change dates, provided that the base operating system provides this information. The command is also used on NIS clients to ensure that the password change information is retrieved from the server.
This chapter provides the hardware and software requirements that must be met to install Tivoli Policy Director for Operating Systems. The information provided here supersedes information provided in the Tivoli Policy Director for Operating Systems Installation Guide.

Hardware Requirements for Installing Tivoli Policy Director for Operating Systems

The memory requirements for a Tivoli Policy Director for Operating Systems machine are provided in the following table.

**Table 1. Memory Requirements**

<table>
<thead>
<tr>
<th>Minimum RAM</th>
<th>64 MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended RAM</td>
<td>128 MB or greater</td>
</tr>
</tbody>
</table>

The Tivoli Policy Director for Operating Systems installation package consists of the following software products:

**PDOS**  Tivoli Policy Director for Operating Systems

**PD**  Tivoli Policy Director

**GSKit**  IBM Global Security Toolkit

**LDAP**  IBM SecureWay Directory Client

These products are installed in different directories based on the operating system platform. The following table outlines the disk space requirements for installing Tivoli Policy Director for Operating Systems and these related products. In addition to the amount of disk space indicated in the table, you should have at least 500 MB of temporary disk space available.

**Table 2. Disk Space Requirements for Installation**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Approximate Space Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>80 MB in <code>/opt</code> for Tivoli Policy Director for Operating Systems and Tivoli Policy Director runtime</td>
</tr>
<tr>
<td></td>
<td>30 MB in <code>/usr</code> for GSKit, and LDAP</td>
</tr>
<tr>
<td></td>
<td>100 MB in <code>/var</code> for Tivoli Policy Director for Operating Systems runtime files</td>
</tr>
<tr>
<td>HP-UX</td>
<td>100 MB in <code>/opt</code> for Tivoli Policy Director for Operating Systems, GSKit, LDAP, and Tivoli Policy Director runtime</td>
</tr>
<tr>
<td></td>
<td>100 MB in <code>/var</code> for Tivoli Policy Director for Operating Systems runtime files</td>
</tr>
</tbody>
</table>
Table 2. Disk Space Requirements for Installation (continued)

<table>
<thead>
<tr>
<th>Platform</th>
<th>Approximate Space Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>100 MB in /opt for Tivoli Policy Director for Operating Systems, GSKit, LDAP, and Tivoli Policy Director runtime</td>
</tr>
<tr>
<td></td>
<td>100 MB in /var for Tivoli Policy Director for Operating Systems runtime files</td>
</tr>
<tr>
<td>Linux</td>
<td>100 MB in /opt for Tivoli Policy Director for Operating Systems, GSKit, LDAP, and Tivoli Policy Director runtime</td>
</tr>
<tr>
<td></td>
<td>100 MB in /var for Tivoli Policy Director for Operating Systems runtime files</td>
</tr>
</tbody>
</table>

Note: For all platforms, space required under /var/pdos is dependent on your policy and audit settings; space required can increase over time.

Supported Operating System Levels and Required Patches

Tivoli Policy Director for Operating Systems is supported on the operating system platforms listed in [Table 3]. In addition, the following operating systems patches must be installed before installing Tivoli Policy Director for Operating Systems. Contact your operating system vendor to obtain the necessary patches.

Table 3. Supported Operating System Levels and Required Patches

<table>
<thead>
<tr>
<th>Operating System and Version</th>
<th>Patches Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 4.3.1</td>
<td>None</td>
</tr>
<tr>
<td>AIX 4.3.2</td>
<td></td>
</tr>
<tr>
<td>AIX 4.3.3</td>
<td>■ X11.adt.motif 4.3.3.1</td>
</tr>
<tr>
<td></td>
<td>■ X11.compat.lib.X11R5 4.3.3.2</td>
</tr>
<tr>
<td></td>
<td>■ bos.adt.prof 4.3.3.3</td>
</tr>
<tr>
<td></td>
<td>■ bos.rte.libpthreads 4.3.3.11, available with patch u470050</td>
</tr>
<tr>
<td></td>
<td>■ bos.rte.install 4.3.3.14 or higher, available as APAR IY08023</td>
</tr>
<tr>
<td>AIX 5.1</td>
<td>■ X11.adt.motif 5.1.0.0</td>
</tr>
<tr>
<td></td>
<td>■ X11.compat.lib.X11R5 5.1.0.0</td>
</tr>
<tr>
<td></td>
<td>■ bos.adt.prof 5.1.0.0</td>
</tr>
<tr>
<td></td>
<td>■ bos.rte.libpthreads 5.1.0.10 or higher and bos.rte 5.1.0.10 or higher, both available as part of Maintenance Level 5100-01.</td>
</tr>
<tr>
<td>HP-UX 11.00</td>
<td>XSWGR1100B.11.00.47.08 General Release Patches</td>
</tr>
<tr>
<td>HP-UX 11.11</td>
<td>PHCO_24402 and PHCO_24400</td>
</tr>
</tbody>
</table>
Table 3. Supported Operating System Levels and Required Patches (continued)

<table>
<thead>
<tr>
<th>Operating System and Version</th>
<th>Patches Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Linux 6.2 (x86)</td>
<td></td>
</tr>
<tr>
<td>kernel rpms supported:</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.2.14-5.0.i586.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.2.14-5.0.i686.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.2.14-5.0.i586.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.2.14-5.0.i686.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.2.19-6.2.7.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.2.19-6.2.7.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.2.19-6.2.7.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.2.19-6.2.7.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.2.19-6.2.12.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.2.19-6.2.12.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.2.19-6.2.12.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.2.19-6.2.12.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>Red Hat Linux 7.1 (x86)</td>
<td>libstdc++-2.95.2-12mdk.i586.rpm</td>
</tr>
<tr>
<td>kernel rpms supported:</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.4.2-2.i586.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.4.2-2.i686.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.4.2-2.i586.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.4.2-2.i686.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.4.9-31.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.4.9-31.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.4.9-31.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.4.9-31.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>Red Hat Linux 7.2 (x86)</td>
<td>libstdc++-2.95.2-12mdk.i586.rpm</td>
</tr>
<tr>
<td>kernel rpms supported:</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.4.7-10.i586.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.4.7-10.i686.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.4.7-10.i586.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.4.7-10.i686.rpm*</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.4.9-31.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-2.4.9-31.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.4.9-31.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>■ kernel-smp-2.4.9-31.i686.rpm</td>
<td></td>
</tr>
</tbody>
</table>
Table 3. Supported Operating System Levels and Required Patches (continued)

<table>
<thead>
<tr>
<th>Operating System and Version</th>
<th>Patches Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SuSE Linux 7.3 (x86)</td>
<td>k_deflt-2.4.10-12.i386.rpm</td>
</tr>
<tr>
<td></td>
<td>k_smp-2.4.10-12.i386.rpm</td>
</tr>
<tr>
<td></td>
<td>libstdc++-2.95.2-12mdk.i586.rpm</td>
</tr>
<tr>
<td>Solaris 2.6</td>
<td>105181-23, 105591-11 and 107733-09</td>
</tr>
<tr>
<td>Solaris 2.7</td>
<td>107171-05</td>
</tr>
<tr>
<td>Solaris 2.8</td>
<td>None</td>
</tr>
</tbody>
</table>

Asterisk (*) indicates packages that are installed by default during the installation process.

Notes:

1. For the Red Hat Linux and SuSE Linux operating systems, only the listed kernel packages are supported by Tivoli Policy Director for Operating Systems. The kernel packages indicated with an asterisk (*) are the kernels that get installed by default during the install process. The other Red Hat packages are updates that are available from Red Hat.

2. The **libstdc++-2.95.2-12mdk.i586.rpm** patch required for all levels of x86 Linux can be found at [http://www.linux-mandrake.com/](http://www.linux-mandrake.com/) and must be installed before installing any of the products for Tivoli Policy Director for Operating Systems. This package adds libraries of a specific version needed by some of the products. For operating systems with higher-numbered versions of libstdc++ already installed (that is, Red Hat 7.1 and 7.2, and SuSE 7.3), this package must be installed using the **--force** option of the rpm install tool.

Software Provided with Tivoli Policy Director for Operating Systems

Tivoli Policy Director for Operating Systems requires the following products, which are included on the installation media, to be installed.

Table 4. Software Provided

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 4.3.1</td>
<td>IBM Global Security Toolkit 3.0.1.120</td>
</tr>
<tr>
<td>AIX 4.3.2</td>
<td>IBM SecureWay Directory 3.1.1.5 Client</td>
</tr>
<tr>
<td></td>
<td>IBM SecureWay Directory 3.1.1.5 Max Crypto Client</td>
</tr>
<tr>
<td></td>
<td>Tivoli Policy Director 3.8.0 Runtime Environment with Fix Pack 2 (3.8-POL-0002) applied</td>
</tr>
<tr>
<td></td>
<td>Tivoli Policy Director for Operating Systems 3.8.0 Runtime Environment</td>
</tr>
</tbody>
</table>
### Table 4. Software Provided (continued)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 4.3.3</td>
<td>IBM Global Security Toolkit 4.0.3.197</td>
</tr>
<tr>
<td>AIX 5.1</td>
<td>IBM SecureWay Directory 3.2.1 Client with efix4 applied</td>
</tr>
<tr>
<td></td>
<td>IBM SecureWay Directory 3.2.1 Max Crypto Client</td>
</tr>
<tr>
<td></td>
<td>Tivoli Policy Director 3.8.0 Runtime Environment with Fix Pack 2 (3.8-POL-0002) applied</td>
</tr>
<tr>
<td></td>
<td>Tivoli Policy Director for Operating Systems 3.8.0 Runtime Environment</td>
</tr>
<tr>
<td>HP-UX 11.00.47</td>
<td>IBM Global Security Toolkit 4.0.3.168</td>
</tr>
<tr>
<td>HP-UX 11.11</td>
<td>IBM SecureWay Directory 3.2.1 Client with efix4 applied</td>
</tr>
<tr>
<td></td>
<td>Tivoli Policy Director 3.8.0 Runtime Environment with Fix Pack 2 (3.8-POL-0002) applied</td>
</tr>
<tr>
<td></td>
<td>Tivoli Policy Director for Operating Systems 3.8.0 Runtime Environment</td>
</tr>
<tr>
<td>Solaris 2.6</td>
<td>IBM Global Security Toolkit 4.0.3.197</td>
</tr>
<tr>
<td>Solaris 2.7</td>
<td>IBM SecureWay Directory 3.2.1 Client with efix4 applied</td>
</tr>
<tr>
<td>Solaris 2.8</td>
<td>Tivoli Policy Director 3.8.0 Runtime Environment with Fix Pack 2 (3.8-POL-0002) applied (PDRT000380-02)</td>
</tr>
<tr>
<td></td>
<td>Tivoli Policy Director for Operating Systems 3.8.0 Runtime Environment</td>
</tr>
<tr>
<td>Red Hat Linux 6.2 (x86)</td>
<td>IBM Global Security Toolkit 4.0.3.197</td>
</tr>
<tr>
<td>Red Hat Linux 7.1 (x86)</td>
<td>IBM SecureWay Directory 3.2-2 Client</td>
</tr>
<tr>
<td>Red Hat Linux 7.2 (x86)</td>
<td>Tivoli Policy Director 3.8.0 Runtime Environment with Fix Pack 2 (3.8-POL-0002) applied</td>
</tr>
<tr>
<td>SuSE Linux 7.3 (x86)</td>
<td>Tivoli Policy Director for Operating Systems 3.8.0 Runtime Environment</td>
</tr>
</tbody>
</table>

**Note:** The correct version of IBM SecureWay Directory furnished with the various versions of the Linux operating systems is Version 3.2-2, as shown in Table 4. The version of IBM SecureWay Directory listed in Table 1 of the Tivoli Policy Director for Operating Systems Installation Guide (on page 4) is incorrect and should also be Version 3.2-2.

### Installation Notes

Before installing Tivoli Policy Director for Operating Systems, review the following notes to determine if they pertain to your installation environment.

**Install Fails on HP-UX Systems with Patch PHCO_22526 Applied**

If patch PHCO_22526 has been applied to an HP-UX system, the installation of Tivoli Policy Director for Operating Systems fails because of an erroneous prerequisite error.

One way to avoid this problem is to uninstall patch PHCO_22526, install Tivoli Policy Director for Operating Systems, and then re-apply patch PHCO_22526.

Another way to avoid the problem is to install Tivoli Policy Director for Operating Systems using the command line and specifying the `-x enforce_dependencies=false` option on the `swinstall` command. You must ensure that all the prerequisites for Tivoli Policy Director for Operating Systems have been met, otherwise unpredictable results might occur.
Install of IBM SecureWay Directory Client Might Fail

If the install of the IBM SecureWay Directory client on your Tivoli Policy Director for Operating Systems system fails because it is unable to establish communication with the LDAP server, verify that you do not have another LDAP client already installed on the system. Depending on how your operating system was installed, an LDAP client might have been automatically installed which would conflict with the IBM SecureWay Directory client installed and used by Tivoli Policy Director for Operating Systems. To correct the problem, remove the other LDAP client and then reinstall the IBM SecureWay Directory client. For example, some Linux operating systems require the removal of the nss_ldap package (rpm -evf nss_ldap) first.

Patch Required for Tivoli Software Installation Service on Linux

The Tivoli Software Installation Service requires patch 3.7.1-TMF-0009 to be applied in order to install software onto Linux endpoints. Install this patch on the Tivoli management region server and on gateways for Linux endpoints.

Patch Required for Tivoli SecureWay Policy Director Connection Version 3.7

If you plan to install Tivoli Policy Director for Operating Systems on a system that has the Tivoli SecureWay Policy Director Connection Version 3.7 component already installed, you must apply a patch to prevent problems that might occur during distributions and populates. Apply E-Fix PDP37002 or patch 3.7.1-SEC-0006E, or later, to your system.

Applying the patch corrects an incompatibility that exists between the Tivoli SecureWay Policy Director Connection Version 3.7 component and the Tivoli Policy Director Version 3.8 runtime environment, which is installed as part of the installation of Tivoli Policy Director for Operating Systems Version 3.8. No reinstallation or reconfiguration is required after installing the patch.

Upgrade Notes

Before upgrading your existing version of Tivoli Policy Director for Operating Systems, review the following notes to determine if they pertain to your installation environment.

Changes to Initial Policy

Changes were made to the initial Tivoli Policy Director for Operating Systems policy. This is the policy that is defined by default when the first Tivoli Policy Director for Operating Systems system is initially configured, and when the first system is configured in a new policy branch. The changes made to the default policy in this version help establish more distinct roles for Tivoli Policy Director for Operating Systems runtime administrators and auditors. These changes also make it possible to establish native non-root users as Tivoli Policy Director for Operating Systems runtime administrators and auditors and to remove the native root user from being a runtime administrator or auditor.

These changes were not automatically applied during your upgrade of Tivoli Policy Director for Operating Systems. A utility, pdos_defpolicy_update, is provided to help upgrade existing environments to use this new policy. See “Upgrade Considerations After Installing” in the Tivoli Policy Director for Operating Systems Installation Guide for details.
Policy Director Language Packs on Policy Director for Operating Systems NLS Support CD

The Policy Director language packs are shipped on the Tivoli Policy Director for Operating Systems Language Support CD (Native Installation Package, not the Tivoli Installation Package). On AIX, Solaris, and Linux, an executable, `pd_lp`, which is an InstallShield Java package, is provided for installation. For HP-UX, there is a native installation package.

Easy Install Procedure Revised to Include Silent Install

On pages 14–15 of Tivoli Policy Director for Operating Systems Installation Guide, the section titled "Installing On All Platforms Using Easy Install" explains how to use the `ezinstall_pdosrte` script to install and initially configure Tivoli Policy Director for Operating Systems. A revised version of the procedure that includes the steps necessary to perform a silent install follows here.

Installing On All Platforms Using Easy Install

The `ezinstall_pdosrte` script is provided to install and initially configure Tivoli Policy Director for Operating Systems with a minimum amount of effort. The script identifies the components that are already installed, locates the components that must be installed on the installation media, and then installs and configures them. The prerequisite components that are installed automatically by the `ezinstall_pdosrte` process are:

- IBM GSKit
- IBM SecureWay Directory Client
- Tivoli SecureWay Policy Director Runtime

The `ezinstall_pdosrte` process can be run by one of the following methods:

- interactive mode, where the process prompts the user for configuration values
- silent mode, where a response file containing the answers to all of the configuration questions
- combination mode, where some of the response file options are left empty causing `ezinstall_pdosrte` to prompt the user for input. When input is gathered, the process continues in a silent mode fashion.

Interactive Mode

By default, the `ezinstall_pdosrte` script runs in interactive mode. To install using Easy Install in the interactive mode, do the following:

1. Insert the Tivoli Policy Director for Operating Systems (128-bit), Version 3.8 (Native Installation Package) CD into the CD-ROM drive.
2. Log in as root.
3. Mount the CD-ROM drive based on the mounting procedure for your operating system platform.

   Note: On HP-UX, remember that the `pfs_mount` command requires the `pfs_mountd` and `pfss` daemons to already be running.

5. Run the script by entering the appropriate command on the command line, based on your operating system platform:
Linux ./ezinstall_pdosrte.linux

All other platform
./ezinstall_pdosrte

Easy Install prompts you for the information it needs as it runs. After the script completes, Tivoli Policy Director for Operating Systems, as well as the prerequisite software residing on the same machine, have been installed and configured.

Note: Easy Install does not upgrade the language packages installed on the system. You must install the necessary language support using the procedures outlined in either the Native Install or Tivoli Desktop Install sections of the *Tivoli Policy Director for Operating Systems Installation Guide*.

Silent Mode
To perform a silent mode installation and configuration of Tivoli Policy Director for Operating Systems, specify the following response file on the command line:

ezinstall_pdosrte /tmp/ezresponse

where tmp/ezresponse is the path to the response file.

If you do not specify a response file, the ezinstall_pdosrte script looks for a response file that was automatically generated during an earlier process on the machine. (See "Generated Response File" below.) If the response file is found, you are asked if you want to use it. If you answer yes (Y) to the prompt, the process uses any values it finds in the response file.

If, at any time during the gathering of the configuration values, the process cannot find a required value in the response file, you will be prompted for the information. This enables you to avoid having to store passwords or repeatedly change information in the response file. You simply answer each question when prompted and the process continues on silently.

Generated Response File
The process generates a response file at the end of each execution of the ezinstall_pdosrte script. The generated file is named: /var/tmp/ezinstall_pdosrte.rsp

For security reasons, passwords are not stored in the generated response file. If you want to provide a response file containing the passwords, you must edit the response file and enter the passwords in necessary place(s).

The generated response file can be used as a template for future Easy Install processes on other machines. To complete future installations, you will transfer this file to the next machine, edit the file (if necessary to provide updated information pertaining to the particular machine), then initiate the Easy Install process using this file.

Response File Comments
The ezinstall_pdosrte script expects the following fields in the response file for a successful silent install and configuration. The format of the response file is option=value. Stanza names (the words inside the square brackets) are not required; they are used only for self-documentation.

Here is an example of the ezinstall_pdosrte response file:

```
[POLICY DIRECTOR RUNTIME]
ldap-or-domino = 1
host = ldaphost.tivoli.com
port = 389
master-host = polserv.tivoli.com
ssl-port = 7135
pd-cacert =
```

Version 3.8 Revised 4/29/02
[POLICY DIRECTOR FOR OPERATING SYSTEMS]
ladp-cacert = /etc/gsk/pd_ladpcert.arm
suffix = ou=austin,o=ibm,c=us
branch = d11nhp
sec-master-pwd = secret
rspfile =
prompt-languages = NO

Response File Options and Interactive Screen Prompts
ezinstall_pdosrte requests the following options, which are used with the response file:

- **ldap_or_domino**
  - The only value possible for this release 1, indicating an LDAP registry. If the registry is not going to be LDAP, the **ezinstall_pdosrte** process should not be used.

- **host**
  - The name of the LDAP server

- **port**
  - The LDAP non-SSL port

- **master-host**
  - The host name of the policy server

- **ssl-port**
  - The SSL server port for the policy server

- **pd-cacert**
  - If the Policy Director policy server allows automatic downloading of the pdcacert.b64 file by runtime client machines, this option should be left blank. However, if the policy server does not allow automatic downloading of the pdcacert.b64 file, the fully qualified path to the certificate file should be used.

- **ldap-cacert**
  - The LDAP-extracted certificate filename.
  
  **Note:** If **ezinstall_ldap_server** was used to configure the LDAP server and the default keyfile was used (pd_ldapkey.kbd) with the default password (gsk4ikm), the proper certificate file can be found in the /etc/gsk directory of the LDAP server and is called pd_ladpcert.arm. If the default pd_ldapkey.kbd file is not in use, you must provide the path to the extracted certificate file here.

- **suffix**
  - The LDAP suffix or the DN for GSO database
branch
   The name of the policy branch with which to associate this machine.

sec-master-pwd
   The security master password set during the configuration of the Tivoli Policy
   Director for Operating Systems policy server.

rspfile  Optional response file to be used by the pdoscfg process. This file can be used
to specify additional Tivoli Policy Director for Operating Systems configurable
options. This value is not required and, if left blank, will not be prompted for.

prompt-languages
   If language packages have been placed on the CD, the Easy Install process ask
   the user to select which ones to install. By setting this value to no, you can
   bypass this prompt and accept English by default.

   If a response file contains multiple instances of an option, the first one from the top of the
   file is used. Any text that follows a pound (#) sign is interpreted as a comment.
Software Limitations, Problems, and Workarounds

Limitations and problems encountered during testing that could not be fixed in the final version of the product are outlined in this section, along with any known workarounds. Issues related to internationalized versions of the product can be found in Chapter 5, “Internationalization Notes” on page 25.

Space Errors on Heavily Loaded HP-UX Systems

On heavily loaded HP-UX systems, you might see the following error message generated in the PDOSD log file, /var/pdos/log/pdosd.log:

```
2000-12-01-17:48:32.863+00:00 I----- 0x35A62686 
pdosd ERROR oss db hla_db_hash.c 924 0x00000015
An error occurred while fetching the entry
from the database: key = status = 10.210.3.36 : 12
```

This error message indicates that all of the system-wide address space available for shared data has been consumed. This situation arises when an excessive number of processes are running on the system. Tivoli Policy Director for Operating Systems continues to operate normally in this situation.

AIX NIS Client and Tivoli Policy Director for Operating Systems Startup Order

On AIX systems, if the system is a NIS client, then the NIS client must be started prior to starting Tivoli Policy Director for Operating Systems. This is the default when Tivoli Policy Director for Operating Systems is configured for automatic start at system boot time. If you manually modify the /etc/inittab file after Tivoli Policy Director for Operating Systems is configured, you must ensure that the entry for Tivoli Policy Director for Operating Systems comes after the entry for the NIS client.

Policy Updates Occurring During Configuration Might Cause Errors

The pdoscfg command might fail if policy updates are occurring during the configuration process. This situation might arise if any of the following activities are occurring within the Tivoli Policy Director domain at the same time as the configuration of a new Tivoli Policy Director for Operating Systems system. They are listed in decreasing order of likelihood of causing the configuration to fail:
Performing policy administration while configuring a Tivoli Policy Director for Operating Systems system

Configuring Tivoli Policy Director for Operating Systems on the first system to subscribe to a new policy branch

Unconfiguring a Tivoli Policy Director for Operating Systems on a system specifying the -remove_per_policy on option of the pdosucfg command

Configuring Tivoli Policy Director for Operating Systems as the second or later machine subscribing to an existing policy branch

Unconfiguring Tivoli Policy Director for Operating Systems on a system

If the Tivoli Policy Director for Operating Systems configuration process fails because of concurrent policy updates, an error is recorded in the error log associated with the pdoscfg command, /var/pdos/log/pdoscfg.log. To correct the problem, issue the pdoscfg command again after the conflicting operations have completed.

Server Connections Might Be Lost During Configuration

If the connection to the Tivoli Policy Director management server or LDAP server is lost during the configuration of a Tivoli Policy Director for Operating Systems system, the pdoscfg command might fail with one of the following errors:

Policy Director command name_of_Policy_Director_command failed.

Registering with Policy Director failed with error code 1.

The pdoscfg command might not have been able to roll back some of the committed changes on these servers. If this occurs, subsequent configurations might fail because of this partial configuration. The following commands need to be issued when connections to the Tivoli Policy Director management server and LDAP server are restored:

1. Issue the following command on the system where the configuration failed:

   /opt/PolicyDirector/bin/svrsslcfg –unconfig -f/dev/null –n pdosd \n   –P sec_master_password

   where sec_master_password is your Tivoli Policy Director security master password.

2. If this is the first Tivoli Policy Director for Operating Systems system to specify this policy-branch value, then issue:

   pdadmin> objectspace delete /OSSEAL/policy-branch

   where policy-branch is the name specified for the –branch option of the pdoscfg command.

3. If this is the first Tivoli Policy Director for Operating Systems system to be configured to this Tivoli Policy Director management server, then issue:

   pdadmin> objectspace delete /OSSEAL

4. Retry the configuration command.

pdosucfg Command Completes with Errors

The pdosucfg command completes Tivoli Policy Director for Operating Systems unconfiguration even if errors are encountered during some of the unconfiguration steps. Some manual cleanup might need to be performed to complete the Tivoli Policy Director for Operating Systems unconfiguration.
If the **pdosucfg** command reports that it has completed with errors, check the 
/var/pdos/log/pdosucfg.log file for more information about the specific errors.

If errors were encountered when running the **svrsslcfg** command to unregister with Tivoli Policy Director, on the system where unconfiguration failed, type the following **svrsslcfg** command on the command line:

```
/opt/PolicyDirector/bin/svrsslcfg -unconfig -f /dev/null \
    -n pdosd -P sec_master_password
```

where `sec_master_password` is your Tivoli Policy Director security master password. Ensure that the Tivoli Policy Director management server is operating normally before issuing the command.

If the **-remove_per_policy on** option of the **pdosucfg** command was specified and errors were encountered while unregistering the policy-specific policy information, type the following **pdadmin** command on the command line to complete the policy branch removal:

```
pdadmin> objectspace delete /OSSEAL/policy_branch
```

where `policy_branch` is the name that was specified for the **-branch** option of the **pdosucfg** command. Ensure that the Tivoli Policy Director management server is operating normally before issuing the command.

### Failed Password Changes on AIX Systems Not Audited

Failed attempts to change a password on AIX systems due to system restrictions, such as no matching of old password, are not audited by Tivoli Policy Director for Operating Systems.

### Files Protected with Rename Permission Can Be Renamed on Linux Systems Using mv Command

A file protected with an ACL of **Rename** can be renamed using the **mv** command on Linux. This is caused by the **mv** command on Linux copying the file to the destination directory after the rename operation fails. Using the **rename** command results in the action being denied, as expected.

### Policy Not Enforced on Solaris Systems Using NFS Version 2

Tivoli Policy Director for Operating Systems policy is not enforced for files and directories that reside on volumes mounted using NFS version 2 on Solaris systems. Volumes mounted using NFS version 3 are protected as expected. Files and directories to be protected on Solaris systems should only be mounted using NFS version 3.

### No Trace Events for Processes Started Before Tivoli Policy Director for Operating Systems

As described in the *Tivoli Policy Director for Operating Systems Administration Guide*, trace_file and trace_exec audit events are not generated for processes that were running before Tivoli Policy Director for Operating Systems was started. Try to arrange your start sequence so that Tivoli Policy Director for Operating Systems is started and active before starting processes that you want to monitor.
Trace Events for CDE-Originated Logins Might Be Missed

As described in the Tivoli Policy Director for Operating Systems Administration Guide, trace_file and trace_exec audit events might not be generated for processes that are starting at the same time as Tivoli Policy Director for Operating Systems. This problem can occur on systems where a CDE-originated login occurs after the initialization of Tivoli Policy Director for Operating Systems has started, but before it has completed. To reduce the chance of this occurring, you can change the order that the processes on the system start and perhaps introduce a sleep interval of 30 seconds or more.

PDOS Login Activity Policy on HP-UX 11x with rexec/remsh

The PDOS login activity policy does not work with the HP-UX login programs rexecd and remshd on HP-UX 11.00 levels prior to HP-UX 11.11 (11i). This is a limitation of the HP-UX 11.00 platform because these programs are not PAM-enabled. Other login policy (such as terminal, time of day, holiday) is still applied. Login using rexec or remsh on an HP-UX 11.00 machine should be disabled if there is a need to enforce login activity policy.

These programs are PAM-enabled in HP-UX, release 11.11 (11i), as described in "reecd, remshd - used PAM for authentication" document, under the heading "HP-UX 11i non-critical enhancement impacts" at http://devresource.hp.com/STK/impactlist.html.

Grace Login Behavior is Different on AIX Systems

On AIX systems running in an NIS environment, the handling of grace logins is different than that on other platforms, or on AIX systems where password information is maintained locally. Normally, when a password expires and the grace logins value is set to zero, the user is prompted to change their password upon their next login attempt. However, because AIX does not use Pluggable Authentication Modules (PAM) for authorization, this condition in an NIS environment results in the login attempt being denied. A new password change date must be set for the user before that user can successfully log in.

Cannot Remove the Logfile Adapter During a Distribution

The Tivoli Enterprise Console UNIX logfile adapter cannot be removed from endpoints when an adapter configuration profile, either PDOS-ACPROF or PDOS-RISKMGR-ACPROF, is being updated to remove adapter records and then distributed.

To remove the logfile adapter in this case, do the following:

1. Stop the logfile adapter. This can be done using the Stop TEC Adapter task from the Tivoli desktop.
2. Remove the adapter record in the appropriate adapter configuration profile.
3. Distribute the updated adapter configuration profile.

Logfile Adapter Fails to Start on AIX 5.1 Systems After Reboot

The Tivoli Enterprise Console UNIX logfile adapter can fail to start on AIX 5.1 systems after a reboot. This problem occurs because the /etc/Tivoli/tecad/pdos/bin/init.tecad_logfile file provided with Tivoli Enterprise Console Version 3.7.1 does not handle the AIX 5.1 rname.
To correct the problem, modify the /etc/Tivoli/tecad/pdos/bin/init.tecad_logfile file to add the following four lines after line 168 in the existing file:

```bash
*:AIX:*:5)
INTERP="aix4-r1"
...
```

**Logfile Adapter on Solaris Systems Fails Under Heavy Load**

The Tivoli Enterprise Console UNIX logfile adapter can fail on Solaris systems when the volume of generated audit events is high. If the logfile adapter fails, you can restart it using the **Start TEC Adapter** task from the Tivoli desktop.

**Stopping and Restarting LDAP Server Can Cause Deadlock**

Stopping and subsequently restarting the LDAP server while Tivoli Policy Director for Operating Systems is active could result in a deadlock condition. Tivoli Policy Director for Operating Systems relies on the LDAP services to obtain credentials from the Tivoli Policy Director user registry as well as for access to network resources needed for making an authorization decision.

When Tivoli Policy Director for Operating Systems detects that it has become isolated from the LDAP server, cached credentials are used in making authorization decisions. When connectivity with the LDAP server is reestablished, any credentials that should have been refreshed during the time of the isolation are refreshed.

Depending on the timing between when Tivoli Policy Director for Operating Systems detects communication with the LDAP server has been restored and when the LDAP server accesses network resources during initialization, a situation can occur where the user who is restarting the LDAP server needs to have their credentials refreshed. In this case, a network access request made by the LDAP server could result in a call to Tivoli Policy Director for Operating Systems to make an authorization decision. Tivoli Policy Director for Operating Systems recognizes that it needs to get refreshed credentials for the user making the request and calls the LDAP server, which results in a deadlock because the LDAP server is already waiting for a response from Tivoli Policy Director for Operating Systems on its earlier authorization request.

You can prevent this problem in one of two ways:

1. Add the LDAP server process, `slapd`, to the Immune-Programs list in the Trusted Computing Base (TCB).
   
   If the LDAP server process is immune, no authorization decisions need to be made during initialization, avoiding the deadlock condition.

2. Stop the Tivoli Policy Director for Operating Systems daemons before you restart the LDAP server. After the LDAP server is restarted, restart Tivoli Policy Director for Operating Systems.

---

3. **Software Limitations, Problems, and Workarounds**
Login Activity Policy Might Not Be Enabled After Upgrade

If you are upgrading from a previous version of Tivoli Policy Director for Operating Systems, login activity policy might not be properly enabled after the upgrade is complete. This is caused by the Tivoli Policy Director for Operating Systems Version 3.7 product erroneously indicating that login activity policy is enabled, even though login activity policy support was not included in that level of the product. Login activity policy was made available in a subsequent patch level.

To enable login activity policy enforcement on a system that has been upgraded from Version 3.7, enter the following commands.

```bash
pdoscfg -login_policy off
pdoscfg -login_policy on
```

Considerations When Running on HACMP for AIX Systems

When running on a High Availability Cluster Multiprocessing (HACMP) for AIX system, you need to ensure that the appropriate actions are taken when a system is taken down and rolled over to another system in the HACMP cluster. This is necessary because Tivoli Policy Director for Operating Systems relies on IP addresses when communicating with the LDAP server. In a HACMP pre-event script, shut down Tivoli Policy Director for Operating Systems. In a HACMP post-event script, which runs on the new system, restart Tivoli Policy Director for Operating Systems. This ensures that Tivoli Policy Director for Operating Systems runs in a consistent network environment. Consult the HACMP for AIX documentation for additional details.

Some Tasks Do Not Encrypt Tivoli Policy Director Administrator Password

The following tasks, provided in the Tivoli Policy Director for Operating Systems Management Tasks component, do not hide the Tivoli Policy Director administrator password when it is entered on the display:

- Configure PDOS Server
- Import UNIX Users and Groups
- Migrate TACF to PDOS

This password is subsequently sent over the network to the target machine unencrypted, which could result in the password being intercepted and security being compromised.

Extraneous Text Shown for Hostname in Events in Tivoli Risk Manager

When integrating Tivoli Policy Director for Operating Systems events with Tivoli Risk Manager, Version 3.8, events are displayed with extraneous text in the hostname field. The hostname field displayed might look similar to the following:

```plaintext
<Event Base Class>::<Machine hostname> <Event Source Hostname>::N/A <Destination Hostname>
```

The character string N/A should be ignored.
Uninstall Might Fail on Linux Systems

The uninstall of Tivoli Policy Director for Operating Systems, the Tivoli Policy Director runtime environment, or any rpm package might fail after installing patch rpm-4.0.2-6x.i386.rpm on a Linux system.

If errors are encountered when uninstalling on Linux, rebuild the Linux rpm database using the following command and then try to uninstall again.

```
rpm --rebuilddb
```

Auth Requisite Modules on PAM Platforms

Tivoli Policy Director for Operating Systems login activity policy requires that there be no pluggable authentication module (PAM) auth modules that are \textit{requisite} for login purposes. This means that in the PAM configuration files, no module can have its control flag set to \textit{requisite}. (See documentation on PAM configuration files for more information.) This setting bypasses necessary steps that are performed by the Tivoli Policy Director for Operating Systems login activity PAM module. These modules must have their control flags set to \textit{required}.

Some platforms (for example, SuSE Linux) ship some PAM configuration files that specify auth modules as requisite. These configuration files must be edited and the control flag changed from requisite to required. PAM configuration files vary, depending on the platform: HP-UX and Solaris systems use the \texttt{/etc/pam.conf} file to configure PAM; Linux platforms use files under the \texttt{/etc/pam.d} directory; AIX does not support PAM. Any line in the configuration files that specifies both auth and requisite must be modified to specify auth and required.

Problems Unlocking CDE Screen Lock on AIX Systems after Installation/Configuration

If Tivoli Policy Director for Operating Systems is installed, configured, and started on an AIX system with an active CDE environment that has been screen-locked, attempts to unlock the CDE screen lock might fail. This is due to the fact that, on AIX systems, the CDE-related processes do not fully reevaluate the AIX authentication plug-in configuration files when they are updated while the CDE processes are running. Notably, the \texttt{/usr/lib/security/methods.cfg} file is not reprocessed. As a result, the login (or screen unlock) processing does not complete successfully. This behavior seems to have been introduced in AIX, Version 5, and on the most recent maintenance levels of AIX, Version 4.3.3.

There are two ways to work around this behavior:

- reboot the machine, after the configuration of Tivoli Policy Director for Operating Systems

  OR

- stop (kill -9) all the CDE-related processes and the X server. Then restart CDE with \texttt{/etc/rc.dt start}. Following is an example of this procedure initiated from a remote login window:

  ```
  # ps -efl|grep dt
  root 3922  7228  0 08:49:30 - 0:00 /usr/dt/bin/dtlogin
  root 4206  3922  0 08:49:31 - 0:00 /usr/lpp/X11/bin/X -D /usr/lib/X11//rgb
  -T-force :0 -auth /var/dt/A:0-SUdRia
  root 18736 22978 0 09:13:23 - 0:00 dtgreet
  root 19900  7746  2 09:13:39 pts/0 0:00 grep dt
  ```
Execution of PDOS Tasks without root in osseal-admin

If root is removed from the osseal-admin group, the PDOS Tasks must be modified to run under a user ID that has been added to the osseal-admin group. Several other actions should be taken due to the architecture of Tivoli Management Agent (TMA) task execution. The basic execution of TMR Task on an Endpoint is as follows. Solaris is used in the example, but the steps apply to all platforms.

1. The user runs a task on a Solaris endpoint for the first time.
2. The executable that contains the run_task() method for an endpoint is named task_endpoint. The TMA knows that this is supposed to live at $LCFROOT/dat/1/cache/bin/solaris2/TASA?TASK_LIBRARY/task_endpoint.
3. The TMA checks its cache index to determine if the file exists.
4. Because this is a brand new endpoint install, it does not exist.
5. The TMA contacts the gateway it is connected to and downloads task_endpoint from the gateway’s lcf_bundle directory. It then updates its cache index with unique information about task_endpoint. The information is basically a signature that uses the date of the file.
6. The TMA spawns $LCFROOT/dat/1/cache/bin/solaris2/TAS/TASK_LIBRARY/task_endpoint as root to execute the requested task.
7. Before spawning the actual task, task_endpoint must switch to the user ID under which the task is supposed to run. If a group ID was specified, it must be changed to this ID as well.
8. The user runs the task on the same endpoint again.
9. The TMA checks its cache index, finds task_endpoint, and then requests that the gateway compare the signature to task_endpoint in the gateway’s lcf_bundle directory. If they match, task execution proceeds. If they do not match, meaning that task_endpoint in the gateway’s lcf_bundle is newer (from a patch) than what is in the cache, then the TMA downloads the new task_endpoint and task execution proceeds.

Steps 7 and 9 can cause problems in a PDOS environment. For Step 7, appropriate policy must be implemented to allow task_endpoint to switch to execution ID. This can be accomplished by registering task_endpoint as an impersonator program using /OSSEAL/branch/TCB/Impersonator-Programs/LCFROOT/dat/1/cache/bin/cache/bin/solaris2/TAS/TASK_LIBRARY/task_endpoint

If a new task_endpoint is downloaded, as in Step 9, then task_endpoint becomes untrusted. The pdosbjsig command can be used to retrust task_endpoint.
Considerations When Upgrading the Operating System on a Machine Running PDOS

Upgrading an operating system installation (such as, migrating AIX, Version 4.3.3, to Version 5.1), produces changes to many files. Any operating system file registered in the Tivoli Policy Director for Operating Systems Trusted Computing Base (TCB) that is changed in the upgrade will be marked untrusted when Tivoli Policy Director for Operating Systems is restarted after upgrade. Any executable file that is marked untrusted cannot be executed. For example, the telnetd daemon could be changed during an upgrade. On the first attempt to telnet into the upgraded machine after Tivoli Policy Director for Operating Systems is started, inetd will fail to start telnetd. This is because the pdosd daemon detects that telnetd’s signature has changed and marks it as untrusted. From this point on, telnetd will not be able to execute while Tivoli Policy Director for Operating Systems is running until telnetd is marked trusted again.

To avoid this situation, follow these steps when upgrading the operating system level:

1. Prior to performing an operating system upgrade, it is recommended that you determine if any files registered with the TCB are marked as untrusted. Use the following command:
   ```bash
pdosobjsig -l untrusted
   ```
   If there are files marked untrusted in the TCB, it may indicate that the file has been compromised. Based on the security practices in place, you might want to determine why these files have been marked untrusted prior to performing the operating system upgrade or you might simply keep track of them so that you do not inadvertently mark them trusted after the operating system upgrade.

2. Get a list of all files that are registered in the TCB. Use the following command:
   ```bash
   pdosobjsig -n -l all > tcb.files.output.file
   ```

3. If they are enabled, turn off login activity policy enforcement and autostart, using the following command:
   ```bash
   pdoscfg -login_policy off -autostart off
   ```

4. Stop Tivoli Policy Director for Operating Systems, using the following command:
   ```bash
   rc.osseal stop
   ```

5. Perform the operating system upgrade.

6. Check the signatures of all the files registered in the TCB, using the following command:
   ```bash
   pdosobjsig -c objectname
   ```
   where `objectname` is the name of a file registered in the TCB. Do this for each file in the list obtained in Step 1. Any file that was modified during the upgrade will be marked as untrusted in the TCB when the signature is checked.

7. Mark as trusted all objects that should be trusted.
   If Step 1 did not show any files marked as untrusted prior to the upgrade, or you are satisfied with the files that were marked untrusted and are certain that you want to mark these files as trusted, mark all objects as trusted using the following command:
   ```bash
   pdosobjsig -S trusted
   ```
To have more control over what becomes trusted, you can determine which files are currently untrusted using the following command:

```
pdosobjsig -l untrusted > untrusted.files.list.output.file
```

and review this list of files, along with the detailed information about when and why each file was marked untrusted.

8. Entrust each file individually, using the following command:

```
pdosobjsig -u objectname -s trusted
```

9. Turn on login activity policy enforcement and autostart (if you had turned them off):

```
pdoscfg -login_policy on -autostart on
```

10. Start Tivoli Policy Director for Operating Systems, using the following command:

```
rc.osseal start
```

If Tivoli Policy Director for Operating Systems is still active on the machine, then the user executing these commands must be a member of the Access Manager group, osseal-admin; this is true even if that user is the root user. Natively, the user must either be a member of the native osseal group or be the root user.

If Tivoli Policy Director for Operating Systems is not active on the machine, then the user must either be the root user or be a member of the native osseal group.

**PDOS Login Activity Policy with $HOME/.rhosts and /etc/hosts.equiv**

The use of the system files $HOME/.rhosts and /etc/hosts.equiv is discouraged when PDOS login activity policy is configured because the files are viewed as insecure. The behavior of this configuration depends on the platform. On AIX systems, $HOME/.rhosts and /etc/hosts.equiv completely circumvent PDOS login activity policy with programs that use these files for authentication (rlogin, rsh, and so forth). Other login policy (such as terminal, time of day, holiday) is still enforced. This is a limitation of the AIX platform, as the PDOS authentication plug-in is not invoked when authentication occurs through $HOME/.rhosts and /etc/hosts.equiv.

On pluggable-authentication-module (PAM) platforms, Solaris, HP-UX, and Linux, Tivoli Policy Director for Operating Systems correctly enforces login activity policy, even if the $HOME/.rhosts or /etc/hosts.equiv entries are used during authentication by programs such as rlogin and rsh. If an account is suspended or locked due to login activity policy enforcement, subsequent access will be denied.

**Limitation of the pdosexempt Command**

The pdosexempt command only works for processes that Tivoli Policy Director for Operating Systems is aware of. Tivoli Policy Director for Operating Systems gains awareness when it sees a process start. Processes that exist prior to the first start of Tivoli Policy Director for Operating Systems on a system after a reboot cannot be exempted from authorization policy by the pdosexempt command. Any such process must be restarted so that Tivoli Policy Director for Operating Systems is aware of the process before the pdosexempt command can be used to render that process exempt from policy.
Updates to the documentation that correct errors or remedy omissions are provided in this section. The latest version of the documentation for Tivoli Policy Director for Operating Systems can be found on the Web at [http://www.tivoli.com/support/documents/](http://www.tivoli.com/support/documents/).

### Some pdoscfg Options Incorrectly Documented

A `pdoscfg` option is shown with incorrect parameters in the Tivoli Policy Director for Operating Systems documentation:

- On page 41 of the *Tivoli Policy Director for Operating Systems Installation Guide*, the `-tcb_interval` option is shown as `number_of_minutes`; it should read `number_of_seconds`. The option is correctly documented in Appendix A, "PDOS Configuration Options".

- On page 153 of the *Tivoli Policy Director for Operating Systems Administration Guide*, the `-tcb_interval` option is shown as `number_of_minutes`; it should read `number_of_seconds`. The option is correctly documented in the Options section.

In addition, the `pdoscfg -?` command returns incorrect information indicating that the `-tcb_interval` option is in minutes. However, the `pdoscfg -help` command returns the correct information.

### Additional Information on Task: Subscribe PDOS Endpoints

On page 129, in the *Tivoli Policy Director for Operating Systems Administration Guide*, the following paragraph should be added to the end of the description of the "Subscribe PDOS Endpoints" task:

This task should only be run on the TMR Managed Node. It is not written to be run on an endpoint and interact with Tivoli Policy Director for Operating Systems. It interacts with the TMR database.

### Information about Kill Permission is Incorrect

On page 18, in the *Tivoli Policy Director for Operating Systems Administration Guide*, the first bullet under Table 9 "File Permissions" is incorrect. The information, which describes the special behavior of the Kill permission, includes the File resource name but does not include the File component. The information is also misleading in its claim that this permission can be applied to control the ability to shut down or reboot the system. The bullet should read:
The Kill (K) permission can be applied to the special File resource /OSSEAL/policy-branch/File/unix to control the ability to reboot the system by programs that issue the reboot () system call.

**Command Line Arguments Added to se2pdos Utility**

Two command line arguments were added to the se2pdos utility to simplify the handling of the owner permissions (but omitted from the Tivoli Policy Director for Operating Systems Administration Guide):

- **–no** When this flag is entered on the command line, all owner entries for nobody are ignored.
- **–nO** When this flag is entered on the command line, all owner entries are ignored.

A common technique used in SeOS policy to set up a resource with no owner is to set the owner to nobody when creating the resource. Here is an example:

```plaintext
editres FILE("/.rhosts") audit(FAILURE) defaccess(NONE) warning owner('nobody')
```

When se2pdos processes SeOS resources, it creates an entry in the access control list (ACL) for the SeOS resource owner. For the nobody case, this is not needed in most environments. As an optimization to se2pdos, a command line option was added which caused it to discard the owner (nobody) tags and not create an entry in the ACL for user nobody. This keeps the policy cleaner, more efficient, and helps reduce the size of the Policy Director policy replica.

Because policy is managed centrally by using Policy Director, the owner/manager of that policy is most likely not sec_master, which, by default, has management authority but no OSSEAL permissions. This allows us to discard all owner entries in the policy using the –nO flag.

**Note:** If a user sets –no –nO, the –no flag is silently ignored.
Internationalization Notes

Limitations and problems encountered during testing of internationalized versions of Tivoli Policy Director for Operating Systems which could not be fixed in the final version of the product are outlined in this section, along with any known workarounds.

General Notes

The following general notes apply to one or more internationalized versions of Tivoli Policy Director for Operating Systems.

Language Limitations Involving Non-ASCII Characters

The following limitations apply when you run a Tivoli Policy Director management server and Tivoli Policy Director for Operating Systems in a non-English environment.

- If user data contains characters other than those in the portable character set (7-bit US-ASCII), you must ensure that all Tivoli Policy Director components run using the same code page to properly share data among these components.
- Only the IBM SecureWay Directory server can be used as the user registry when Tivoli Policy Director is configured to run on a non-English system and non-portable character set data creation is required.

Notes Regarding AIX Systems

The following notes apply to AIX systems only.

**PDOSD Daemon Does Not Autostart on AIX Systems**

**LC_MESSAGES=c@lft in /etc/environment**

The PDOSD daemon will fail to start correctly at system boot time on AIX systems where the /etc/environment file contains the lines:

```
LC_MESSAGES=C@lft
export LC_MESSAGES
```

One workaround to this problem is to edit the /etc/environment file and comment out those two lines. After making the change, shut down and reboot the system. The PDOSD daemon should start as expected.

If these lines are necessary for low-function terminals to work correctly in your environment, an alternative workaround is to ensure that LC_ALL is set correctly prior to the PDOSD daemon starting. To accomplish this, write a new script, /usr/local/bin/osseal_init.sh, that contains the following lines:
configuration change needed on some internationalized versions of
red hat linux 7.1

then comment out the original rc.osseal entry in the /etc/inittab file and add a new
entry that calls the new osseal_init.sh script:

# /etc/inittab
(other lines)
:rc.osseal:2:wait:/opt/pdos/bin/rc.osseal start
rc.osseal:2:wait:/tmp/osseal_init.sh

if you use the pdoscfg command to turn off the -autostart parameter, you must do this
workaround when you turn it on again.

notes regarding linux systems

the following notes apply to linux systems only.

configuration change needed on some internationalized versions of
red hat linux 7.1

if you plan to install tivoli policy director for operating systems on a red hat linux 7.1
system running in one of the following locales, you must change a configuration file before
installing.

- japanese (eucjp) (ja_JP.eucjp)
- traditional chinese (zh_TW)

edit the /etc/ld.so.conf file and add the following line:

/usr/lib/gconv

this change corrects a problem caused by the implementation of the iconv character set
conversion interface.

japanese locale and language setting supported on linux systems

the only supported locale and language setting for japanese is ja_JP.eucjp. for example:

LANG=ja_JP.eucjp
LC_ALL=ja_JP.eucjp

Note: Notice the case used in the locale name of ja_JP.eucjp. Using a locale name with
different case, such as ja_JP.eucJP, does not work.

japanese sjis is not currently supported.

Tivoli Policy Director Considerations When Using International
Locales on Linux Systems

The section describes setting up Tivoli Policy Director on Red Hat Linux 7.1 using
international locales. The information is appropriate for Japanese EUC and Traditional
Chinese (BIG5). Japanese SJIS is not currently supported.

1. Install Red Hat Linux 7.1 with Japanese and Traditional Chinese support and with
   XWindows System Configure X, Launch X.
2. Install the PDRTE package.
3. Install the Tivoli Policy Director Language pack:
   # ./pd_lp
4. Configure the PDRTE against a PDMgr that also supports the required locale.

**For Japanese EUC:**

1. Run the following commands:
   ```
   # export LC_ALL=ja_JP.eucjp
   # export LANG=ja_JP.eucjp
   # rxvt -km eucj &
   ```
2. In the rxvt terminal, load pdconfig and ensure that the configuration menu appears in Japanese.

**For Traditional Chinese:**

An additional package that contains the necessary fonts is required. These fonts are not included with Red Hat Linux 7.1.

1. Run the following commands:
   ```
   # rpm -i cxterm-5.1p1-2.i386.rpm
   # export LANG=zh_TW
   # export LC_ALL=zh_TW
   # cxterm -big5
   ```
2. In cxterm, load pdconfig and ensure that the configuration menu appears in Chinese.

The cxterm package can be downloaded from the following Web address:


**Notes Regarding Solaris Systems**

The following notes apply to Solaris systems only.

**Setting the Locale for CDE Login on Solaris 2.8**

There is a known problem when using CDE login on a Solaris 2.8 system where the LC_MESSAGES variable is not set to the specified language chosen from the options button.

After a desktop login on a Solaris 2.8 system, if you do not see messages in the expected language, the locale specific environment variables might not be set correctly. This is a known problem on Solaris 2.8 and is addressed by Solaris patch 109778. The workaround for this problem is to explicitly set the locale specific environment variables to the correct values. For example, if you are using Brazilian-Portuguese, set the following variables to the pt_BR locale:

- LANG=pt_BR
- LC_ALL=pt_BR