SGI™ Internet Server Administrator's Guide

007–4262–002

CONTRIBUTORS

Written by Lori Johnson

Production by Susan Gorski

Edited by Rick Thompson

Illustrated by Chris Wengelski

Engineering contributions by Bao Phac Do, Jim Dethlefson, Anietie Ekanem, Kirk Erickson, Rafael Seidl, Mary Sprowl, Ken Trant

Cover design by Sarah Bolles, Sarah Bolles Design, and Dany Galgani, SGI Technical Publications.

Record of Revision

Version	Description
001	February 2000 Original publication
002	April 2000 Corrections to the ISE 1.0 released version

Contents

Figures

Tables

About This Guide

This publication documents the Internet Server Environment software for the SGI Internet Server. ISE is a set of security and management tools targeted at Internet Service Provider (ISP) customers.

Related Publications

The following documents contain additional information that may be helpful:

- *SGI Internet Server Start Here*
- *SGI 1200-Family of Servers Quick Start Guide*
- *SGI 1200-Family of Servers Errata*
- *SGI 1200-Family of Servers User's Guide*
- *SGI Internet Server Administrator's Guide*
- *SGI ProPack 1.3 for Linux Start Here*
- SGI Linux Web site: `http://oss.sgi.com/projects/sgilinux`

Obtaining Publications

The *SGI Internet Server Administrator's Guide* (`ISE_AG`) and *SGI Internet Server Start Here* (`ISE_SH`) are found in the following locations on an installed system:

- HTML in:

  `/usr/doc/sgi/ise-`*Version*`/ISE_AG-`*Revision*`/html`
  `/usr/doc/sgi/ise-`*Version*`/ISE_SH-`*Revision*`/html`

- PDF in:

  `/usr/doc/sgi/ise-`*Version*`/ISE_AG-`*Revision*`/pdf`
  `/usr/doc/sgi/ace-`*Version*`/ISE_SH-`*Revision*`/pdf`

- Compressed PostScript in:

  /usr/doc/sgi/ise-*Version*/ISE_AG-*Revision*/ps
  /usr/doc/sgi/ise-*Version*/ISE_SH-*Revision*/ps

For example:

```
/usr/doc/sgi/ise-1.0/ISE_AG-001/html
```

Note: Documentation is available on the CD-ROM in `/mnt/cdrom`, rather than `/usr`.

To download a free copy of the Acrobat PDF reader, see:

```
http://www.adobe.com/products/acrobat/readstep.html
```

To obtain the latest SGI documentation, go to the SGI Technical Publications Library at:

```
http://techpubs.sgi.com
```

Conventions

The following conventions are used throughout this document:

Convention	Meaning
`command`	This fixed-space font denotes literal items such as commands, files, routines, path names, signals, messages, and programming language structures.
variable	Italic typeface denotes variable entries and words or concepts being defined.
`user input`	This bold, fixed-space font denotes literal items that the user enters in interactive sessions. Output is shown in nonbold, fixed-space font.

[ ]	Brackets enclose optional portions of a command or directive line.
...	Ellipses indicate that a preceding element can be repeated.

Reader Comments

If you have comments about the technical accuracy, content, or organization of this document, please tell us. Be sure to include the title and document number of the manual with your comments. (Online, the document number is located in the front matter of the manual. In printed manuals, the document number can be found on the back cover.)

You can contact us in any of the following ways:

- Send e-mail to the following address:

  `techpubs@sgi.com`

- Use the Feedback option on the Technical Publications Library World Wide Web page:

  `http://techpubs.sgi.com`

- Contact your customer service representative and ask that an incident be filed in the SGI incident tracking system.

- Send mail to the following address:

  Technical Publications
  SGI
  1600 Amphitheatre Pkwy., M/S 535
  Mountain View, California 94043–1351

- Send a fax to the attention of "Technical Publications" at +1 650 932 0801.

We value your comments and will respond to them promptly.

Introduction

The SGI Internet Server is a completely integrated solution based on the SGI 1200 Linux thin server platform and the Internet Server Environment (ISE) software. The ISE collection of applications and documentation is designed to make your SGI Linux server easier to deploy and operate in demanding and generally insecure Internet environments.

The SGI Internet Server offers the following:

- Easy setup and installation tools
- Management, monitoring, and security tools
- Basic services for Web serving and messaging

All of the software you will need is already preinstalled on your system hard drive. However, if you should need to reinstall from CD later on, see the instructions in the *SGI Internet Server Start Here*. (If you did not receive the ISE CD-ROM set, please contact your sales representative.)

How to Use this Guide

This document is a guide for bringing your SGI Linux server into production as a web-hosting platform. If you intend to use the system for another service, you may want to skip parts of Chapter 3, "Web Hosting Service Setup", page 5, and Chapter 4, "Performance Management with Performance Co-Pilot (PCP)", page 11. If you intend to deploy the system on a network you consider already sufficiently secure, you may want to skip Chapter 5, "Intrusion Detection Using Tripwire", page 21, and Chapter 6, "Suggestions for Secure Server Operations", page 27.

The target audience for this document is production system administrators with at least some familiarity with UNIX or Linux. However, a moderately experienced system administrator more familiar with other operating systems (such as Windows NT) should have little difficulty in mastering the information in this guide.

Support

For SGI Linux support services, see:

`http://support.sgi.com/linux`

General Product Feedback

For general feedback (not support) about the SGI Internet Server, see:

`http://www.sgi.com/cgi-bin/feedback/`

For marketing information, see:

`http://www.sgi.com/solutions/broadband/sgi_internet.html`

Enhancing Web Server Performance

To activate the enhanced Apache Web server with SGI performance improvements, do the following:

1. Log in as `root` or use the `su`(1) command to switch to `root`.
2. Change to the `apache` directory:

   # **cd /usr/sgi/ise/apache**

3. Run the `INSTALL` script:

   # **./INSTALL**

   This script will rebuild Apache and install the improved performance changes. Apache will be restarted at the end of the script and be ready for use.

For more information about the changes applied to Apache, see the following URL:

`http://`*hostname*`/manual/misc/perf-mja.html`

You can find other information about Apache at the following URLs:

`http://`*hostname*`/manual`
`http://`*hostname*`/manual/misc/`

Web Hosting Service Setup

This chapter discusses the following:

Note: The instructions in this chapter assume that you already have network access to Linuxconf on the machine being configured to host the virtual servers.

You can do this by selecting **Launch Linuxconf** from the SGI Internet Server Web administration graphical user interface (GUI) **Management** Web page or by pointing your browser to `http://`*hostname*`:98/`.

Configuring a Virtual Web Server

Virtual servers are used for hosting multiple Web sites using the same instance of the same software; the pages reside in different subdirectory trees.

This section covers the following:

Domain Name Service (DNS) Entries

Both hardware and software virtual servers require that entries be made to the DNS server(s) used by any client wishing to connect to a given virtual server:

- Hardware virtual servers require that a name be assigned to any new IP addresses if you intend to allow named access to those addresses.
- Software virtual servers require that a `CNAME` record be added to the DNS before you can access the server from a virtual name.

Hardware Virtual Servers

Do the following:

1. At the Linuxconf main Web page, select the **Start** button.
2. Select the following links in order:

   Networking
   IP Aliases for virtual hosts
   Select the appropriate network device

3. Enter one or more IP addresses and, optionally, appropriate netmask(s).
4. Select the **Accept** button.
5. Select the following links in order:

   Linuxconf 1.xx xxxx *(upper left corner of page)*
   Control panel
   Activate configuration
   Activate the changes

6. Test your changes

Software Virtual Servers

To set up a name-based (non-IP) virtual Web server in Apache, do the following:

1. At the Linuxconf main Web page, select the **Start** button.
2. Select the following links in order:

   Networking
   Apache Web Server
   Virtual domains

3. Select **Add** button.

4. Enter the following values, at minimum:

Virtual host name:	IP address of server.
Server name:	Fully qualified virtual domain/server name. Note that this is the alias name put into a `CNAME` record on the DNS.
Server aliases:	The hostname and any aliases, without the domain, should be put here. For example: If the virtual server name is `bleezer.woggo.net`, then add `bleezer` here, plus any other shortened names by which you intend for people to access the server. Note that this assumes the appropriate entries in the DNS.
Document root:	The relative or absolute directory from which the virtual server's documents are served.

5. Select **Accept** button.

6. Select the following links in order:

Linuxconf 1.*xx xxxx (near top of page on left side.)*
Control panel
Activate configuration
Activate the changes

7. Test your changes.

Configuring a POP-Only E-mail Account

To create a post-office (POP) email account, do the following:

1. At the Linuxconf main web page, select the **Start** button.
2. Select the following links in order:

   Users accounts
   POP accounts (mail only)

3. Select the **Add** button.
4. Fill in at least the login name and full name fields on the **User account creation** page.
5. Select the **Accept** button.
6. Enter the new user's password, then select the **Accept** button.
7. Reenter the password to confirm it, then select the **Accept** button.
8. Select the following links:

   Linuxconf 1.16 (subrev 1-3) ***(upper left corner of page)***
   Control panel
   Activate configuration
   Activate the changes

Configuring an FTP-Only User Account

To allow your hosted customers to manage the content of their site, you must provide a means for uploading files to your server and deleting files on your server.

One common mechanism is FTP uploads. To enable these for your users, you must do the following:

- Add regular user accounts. For the home directory, specify the document root of the virtual server you created for this hosted customer. For example, `/home/httpd/html/foobar` for the virtual server `www.foobar.com`.
- open up ports 20 and 21 in the `INPUT` chain for `ipchains`(8). See the information about Bastille in *SGI Internet Server Start Here*.

Security recommendations:

- Unless you are planning to allow anonymous access to your FTP server, you should delete the predefined `ftp` account.
- Use the predefined `ftp` group for the hosted accounts
- Ensure that the home directories of the hosted accounts are owned by them and group `ftp`. Files inside the home directories must be readable by the web server user (typically `nobody`). Subdirectories must be readable and executable by the web server user.
- Unless you intend to allow the execution of CGI scripts that capture user data into files stored in the hosted account home directories, it is not necessary to give the web server user write permissions in any directory owned by hosted customer.
- Modify the `/etc/inetd.conf` file to launch the `ftpd`(8) server with the option `-u 0022`. This ensures that newly uploaded files and subdirectories will be created such that only the hosted account owner, and the superuser, can modify or delete them.
- Consider modifying `/etc/inetd.conf` to launch the `ftpd` server with the option `-r` , with `docroot` representing the global document root for the web server (typically `/home/httpd/html`). This ensures that each invocation of the `ftpd` server is confined to a `chroot`(8) prison and attacks based on hosted accounts cannot ever affect parts of the file system other than `docroot`.

For proper operation of a changed-root FTP server, you must provide copies of `ls`(1) and other commands in the appropriate subdirectories of the `chroot` prison. See the `ftpd`(8) man page for instructions in the analogous case of anonymous `ftp` access.

Performance Management with Performance Co-Pilot (PCP)

Performance Co-Pilot (PCP) is a framework and set of services that support system-level performance monitoring and performance management.

In the ISE product, the PCP configuration has been customized to produce Web-based reports generated by PCP tools running in the background. These reports are available from the Internet Server Web administration GUI. These reports are updated in real-time to display short-term and long-term Web server activity and utilization.

This chapter discusses the following:

Performance Status Reports

This section discusses the following:

Accessing the Latest Reports

To access the performance status reports, see the **Monitoring** section of the SGI Internet Server Web administration interface using the following URL:

`http://`*`hostname`*`/sgi-iserver/pcp/management.html`

From the **Monitoring** section, you can select one of the following:

- **last hour** displays detailed performance statistics over the last hour. This report is updated every minute.

- **last day** displays a summary of statistics over the last 24 hours. This report is updated every 15 minutes.

You can access the latest reports directly by using the following URLs:

`http://`*`hostname`*`/sgi-iserver/pcp`
`http://`*`hostname`*`/sgi-iserver/pcp/ISE-1hour.gif`
`http://`*`hostname`*`/sgi-iserver/pcp/ISE-24hour.gif`

Accessing Older Reports

The status reports are placed in the following directory:

`/home/httpd/html/sgi-iserver/pcp`

This directory contains all existing previous reports, which include the hour or day of the week in the file name. The hourly images are named as follows:

- `snap_h`*`HH`*`.gif` for the hourly images, where *HH* is a value from `00` (midnight) through `23` (2300 hours, or 11:00 PM). For example, `snap_h18.ISE-24hour.gif` was created at 6:00 PM. The file will contain data from the previous hour.
- `snap_d`*`DD`*`.gif` for the daily images, where *DD* is a value from `00` (Sunday) through `06` (Saturday). For example, `snap_d03.ISE-24hour.gif` was created on Wednesday. The file will contain data from the previous 24 hours.

There will be 24 `ISE-1hour.gif` files, the oldest of which is overwritten every hour. There will be 7 `ISE-24hour.gif` files, the oldest of which is overwritten every 24 hours.

Report Contents

Figure 4-1 shows an example report.

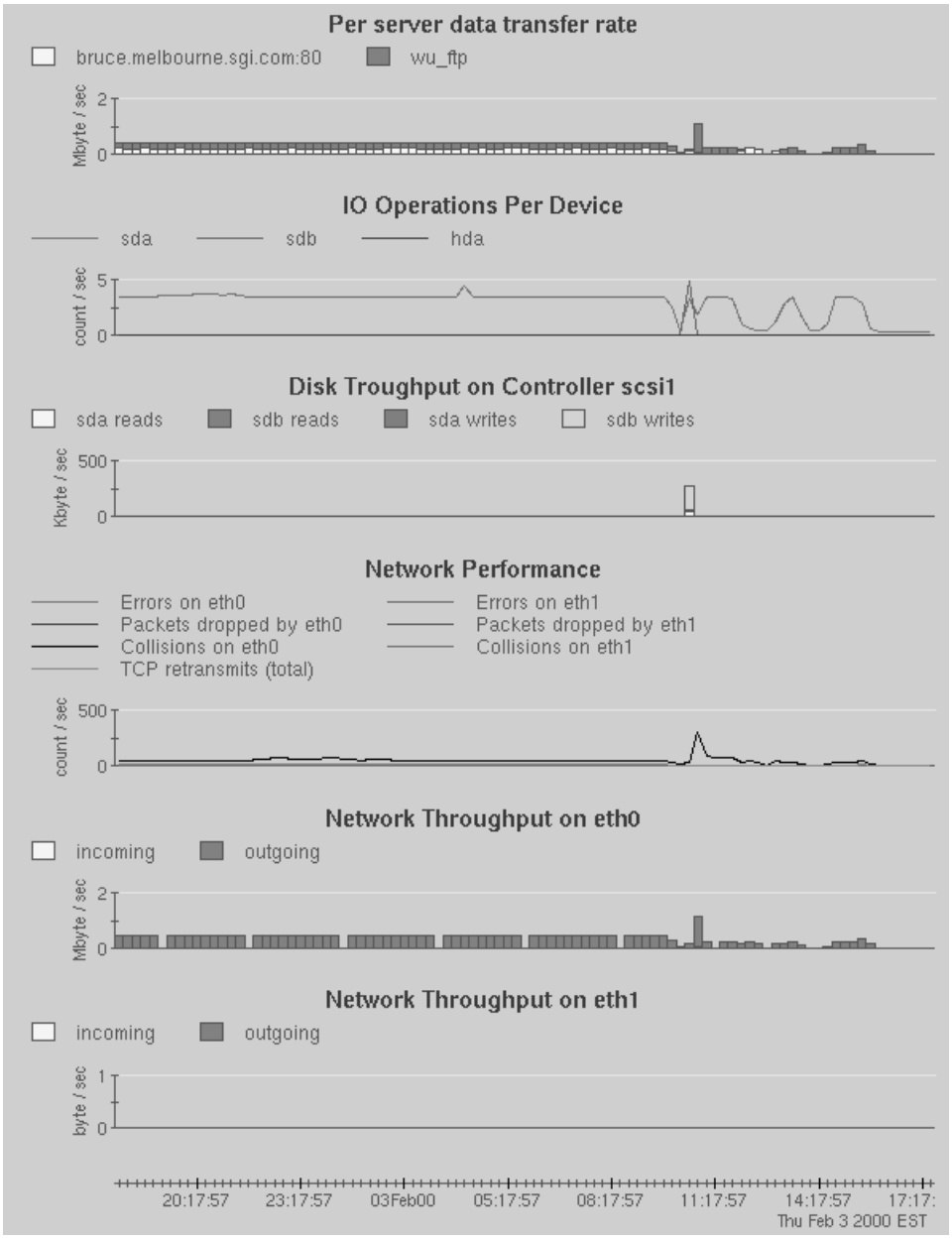

Figure 4-1 Example Last Day Report

These images show various charts with a common time-axis. The following subsections describe each chart.

Per Server Data Transfer Rate

The **Per server data transfer rate** chart shows the data throughput for each `www` and `ftp` server configured on the system as a stacked bar chart. The total height of the bars represents aggregate data throughput for all servers on this host. The chart provides automatic scaling, hence the units on the Y-axis may represent a scale from bytes to Gbytes according to the current traffic.

IO Operations Per Device

The **IO Operations Per Device** chart shows disk input/output (I/O) operations per disk device. All SCSI and IDE disks are included in this chart. The rate of disk I/O operations is strongly correlated with device throughput and the I/O rate may be used as a general indication of device saturation. A high I/O rate on a particular device while others remain relatively idle indicates an imbalance in the I/O load across all devices.

Disk Throughput on Controller *controller_name*

The **Disk Throughput on Controller *controller_name*** chart shows actual data transfer rates for each SCSI device, with one chart for each SCSI controller in the system. Each chart shows a stacked bar, with one component for reads and one component for writes, repeated for each device on the particular SCSI controller. The total height of the stacked bar indicates the total disk traffic throughput on that controller.

A particular controller showing a lot of traffic while others remain relatively idle indicates an imbalance in the I/O load across the system. If disk throughput is perceived to be a performance bottle-neck, an improvement may be gained by spreading the load more evenly across the available controllers; that is, by moving one or more disks to a different controller or moving one or more filesystems to different disks.

Network Performance

The **Network Performance** chart shows the rate of errors, collisions, and dropped packets for each network interface configured in the system (other than serial/modem lines). The Transmission Control Protocol (TCP) packet retransmission rate is also shown in total for all network interfaces.

A high rate of collisions indicates contention for local area network bandwidth with other systems. It is normal to see a small number of collisions, usually in bursts. However, you should investigate a sustained, high rate of collisions.

High rates of dropped packets, errors, or TCP retransmissions indicate poor Web server performance and/or network problems requiring investigation.

Network Throughput on *interface_name*

The **Network Throughput on *interface_name*** chart shows actual network transfer rates for each network device (other than serial/modem interfaces), with one chart for each network interface configured in the system. Each chart shows both incoming and outgoing traffic as a stacked bar, with the total height of the bar indicating total throughput. The following indicate problems:

- Sustained traffic near the available bandwidth indicates that the system is overloaded by client connections. In this situation, most users will be experiencing poor service.
- Unexpectedly low traffic indicates that there may be failing network cables and/or hardware errors. In this situation, users will be experiencing very poor service or no service at all.

PCP Administration

This section discusses the following:

Note: The PCP configuration for ISE requires the following packages, which are preinstalled on your system:

- `pcp` 2.1.3–1 or later
- `pcp-pro` 2.1.2–2 or later
- `pcp-ise` 1.0.0–2 or later

The PCP application generating the report images also requires that the XFree Virtual Framebuffer Server (`XFree-xvfb*.rpm`) is installed; XFree is provided with most base Linux distributions.

Changing the Reports

You can add new reports or change the report contents by adding or changing files ending in `.options` in the `/var/pcp/config/pcp-ise` directory. Each file ending with the `.options` suffix specifies the command line options that are passed to `pmchart`(1), which is the tool used to generate the images. In particular, you can use the `-h` option to tell `pmchart` to monitor a remote host (such as another Web server in your environment that has the PCP RPMs installed). The available options for `pmchart` are fully described in the `pmchart`(1) man page.

Note: If you use the `-h` option to `pmchart`(1), you must open up the appropriate ports in your `ipchains`(8) configurations on both systems. In addition, note that the PCP reports produced with the Web administration GUI. will always feature the name of the local systems. Because this could cause confusion, SGI does not recomment using the `-h` option with the GUI.

If you add, change, or remove files from the `/var/pcp/config/pcp-ise` directory, you must restart `pcp-ise` with the following command:

```
# /etc/rc.d/init.d/pcp-ise restart
```

Changing the Web Configuration

If you change your Web configuration in any of the following ways, you must reinstall the `weblog` Performance Metrics Domain Agent (PMDA) and restart the `pcp-ise` package:

- Add a Web or `ftp` server
- Delete a Web or `ftp` server
- Relocate server activity logs

To reinstall `weblog` and restart `pcp-ise`, enter the following (in the `bash`(1) shell):

```
# cd /var/pcp/pmdas/weblog
# export QUIET_INSTALL=Y
# ./Install
# /etc/rc.d/init.d/pcp-ise restart
```

Real-Time and Remote Display

The performance reports produced by PCP for ISE are configured to work "out of the box", with no user setup normally required. However, you can also use PCP interactively to examine the performance of your Web serving environment in real-time.

You can use PCP interactively by remotely logging in to the server and displaying back the monitoring information to your remote workstation, as shown in Figure 4-2.

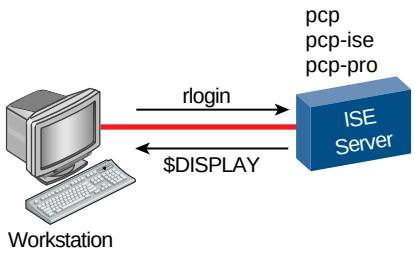

Figure 4-2 Real-Time and Remote Display

For more information about using PCP interactively, see the documentation listed in "For More Information about PCP", page 19.

Real-Time and Remote PCP Installation

You may want to install the `pcp`, `pcp-ise`, and `pcp-pro` packages on a workstation in addition to the SGI Internet Server. Doing so will result in better display performance, especially if the workstation has hardware accelerated graphics. Figure 4-3 shows this deployment.

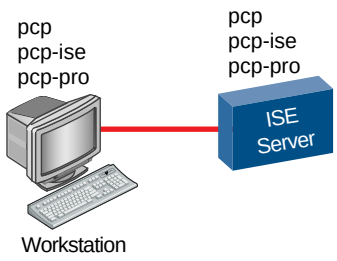

Figure 4-3 Real-Time and Remote PCP Installation

Note: PCP also requires that the XFree Virtual Framebuffer Server (`XFree-xvfb*.rpm`) is installed on the workstation; XFree is provided with most base Linux distributions.

To install the required packages on a Linux workstation, do the following:

1. Log into the workstation as `root`.
2. Insert the ISE CD-ROM in the workstation's driver.
3. Mount the CD-ROM by entering the following:

   ```
   # /bin/mount /dev/cdrom /mnt/cdrom
   ```

4. Change to the `/mnt/cdrom` directory:

   ```
   # cd /mnt/cdrom
   ```

5. Enter the following to install the packages :

   ```
   # rpm -i /mnt/cdrom/RPMS/XFree86-Xvfb*.i386.rpm
   # rpm -i /mnt/cdrom/RPMS/pcp*.i386.rpm
   ```

After the RPMs are installed, the PCP daemons will start automatically on each reboot.

Note: To manually start the PCP daemons, enter the following:

```
# /etc/rc.d/init.d/pcp start
# /etc/rc.d/init.d/pcp-ise start
```

To monitor other performance metrics, you can use live-mode PCP tools such as `pmchart`(1) and `pmgsys`(1). For the Web-centric setup, `weblogvis`(1) and `webvis`(1) provide 3D visualizations of server resource utilization and Web server activity.

You can use the configuration file for `pmchart` to display the same information as shown on the Web page; you can also use it to monitor the metrics at a different sampling rate or do live monitoring. Use the following command:

```
$ pmchart -c ISE
```

The PCP monitoring tools that use a 3D display (`mpvis`, `dkvis`, `osvis`, `webvis`, and `weblogvis`) will work best if there is a 16 bpp or better visual available. An 8 bpp visual will still work, but some annoying colormap flashing may occur. You can use the `xdpyinfo` tool to determine what visuals are available.

For More Information about PCP

Refer to `http://oss.sgi.com/projects/pcp` for additional information. Also see the following `README` files:

`/usr/doc/pcp-`*Version*`/README`
`/usr/doc/pcp-ise-`*Version*`/README`
`/usr/doc/pcp-pro-`*Version*`/README`

If you want to use PCP for interactive performance analysis, see the *Performance Co-Pilot User's and Administrator's Guide*. If you want to develop your own performance monitoring tools or agents, read the *Performance Co-Pilot Programmer's Guide*. Both of these books are available online from the SGI Technical Publications Library: `http://techpubs.sgi.com`.

These documents describe the IRIX version of the PCP product, which differs only slightly from the Linux version. Table 4-1 summarizes the differences.

Table 4-1 PCP Differences between IRIX and Linux

Directory	IRIX	Linux
`rc`/`startup` scripts	`/etc/init.d`	`/etc/rc.d/init.d`
Private PCP binaries	`/usr/pcp/bin`	`/usr/share/pcp/bin`
Shared PCP files (shareable for diskless)	`/usr/pcp`	`/usr/share/pcp`
Directory of man pages	`/usr/share/catman`	`/usr/man`
PCP logs	`/var/adm/pcplog`	`/var/log/pcp`
PCP documentation	`/var/pcp`	`/usr/doc/pcp-`*Version*
Directory for PCP demos and examples	`/var/pcp/demos`	`/usr/share/pcp/demos`
`magic`, as used by `file`(1)	`/etc/magic`	`/usr/share/magic`

The version of PCP packaged with the SGI Internet Server includes features that are derived from the IRIX version of PCP. For more information, see: `http://www.sgi.com/software/co-pilot`.

Intrusion Detection Using Tripwire

Tripwire is a tool for *file integrity assessment*, a form of intrusion detection that works in conjunction with other security technologies. Tripwire scans a computer system and creates a database of files that contain a compact snapshot of the system in a known state. Once this baseline database is created, you can run an integrity check at any time to detect and report changes to the system.

This chapter discusses the following:

Installing Tripwire

This section tells you how to install Tripwire and provides an example.

Tripwire Installation Procedure

To install Tripwire, do the following:

1. Log in as `root` or use the `su`(1) command to switch to `root`.
2. Change to the `tripwire` directory:

   # **`cd /usr/sgi/ise/tripwire`**

3. Run the `install.sh` script:

   # **`./install.sh`**

4. Press `Enter` to view the license agreement. After reading it, enter `accept` to accept it.
5. Enter site and local keyfile passphrases (passwords) as prompted.

Tripwire Installation Example

The following shows an example of the Tripwire installation process. The license agreement text has not been fully reproduced. For your own security, use your own passphrases rather than those shown in this example.

```
# cd /usr/sgi/ise/tripwire
# ./install.sh
Installer program for:
Tripwire(R) 2.2.1 for Unix

Copyright (C) 1998-2000 Tripwire (R) Security Systems, Inc.  Tripwire (R)
is a registered trademark of the Purdue Research Foundation and is
licensed exclusively to Tripwire (R) Security Systems, Inc.


LICENSE AGREEMENT for Tripwire(R) 2.2.1 for Unix

Please read the following license agreement.  You must accept the
agreement to continue installing Tripwire.

Press ENTER to view the License Agreement. <Enter_key>

                  END USER SOFTWARE LICENSE AGREEMENT

This Tripwire Security Systems, Inc. ("Tripwire") End-User License
...
[Text deleted from the example]
...

Please type "accept" to indicate your acceptance of this  accept
Using configuration file install.cfg

Checking for programs specified in install configuration file....

/usr/lib/sendmail exists.  Continuing installation.

/bin/vi exists.  Continuing installation.

This program will copy Tripwire files to the following directories:

       TWROOT: /usr/TSS
```

```
        TWBIN: /usr/TSS/bin
        TWMAN: /usr/TSS/man
     TWPOLICY: /usr/TSS/policy
     TWREPORT: /usr/TSS/report
         TWDB: /usr/TSS/db
 TWSITEKEYDIR: /usr/TSS/key
TWLOCALKEYDIR: /usr/TSS/key

CLOBBER is false.


-----------------------------------------------
Creating directories...
/usr/TSS: created
/usr/TSS/bin: created
/usr/TSS/policy: created
/usr/TSS/report: created
/usr/TSS/db: created
/usr/TSS/key: created
/usr/TSS/key: already exists
/usr/TSS/man: created

-----------------------------------------------
Copying files...
/usr/TSS/bin/siggen: copied
/usr/TSS/bin/twprint: copied
/usr/TSS/bin/twadmin: copied
/usr/TSS/bin/tripwire: copied
/usr/TSS/policy/policyguide.txt: copied
/usr/TSS/policy/twpol.txt: copied
/usr/TSS/man/man4/twconfig.4: copied
/usr/TSS/man/man4/twpolicy.4: copied
/usr/TSS/man/man5/twfiles.5: copied
/usr/TSS/man/man8/siggen.8: copied
/usr/TSS/man/man8/tripwire.8: copied
/usr/TSS/man/man8/twadmin.8: copied
/usr/TSS/man/man8/twintro.8: copied
/usr/TSS/man/man8/twprint.8: copied
/usr/TSS/README: copied
/usr/TSS/Release_Notes: copied
/usr/TSS/License.txt: copied
```

```
-----------------------------------------------
The Tripwire site and local passphrases are used to
sign a variety of files, such as the configuration,
policy, and database files.

Passphrases should be at least 8 characters in length
and contain both letters and numbers.

See the Tripwire manual for more information.

-----------------------------------------------
Creating key files...

(When selecting a passphrase, keep in mind that good passphrases typically
have upper and lower case letters, digits and punctuation marks, and are
at least 8 characters in length.)

Enter the site keyfile passphrase: wgEci99!
Verify the site keyfile passphrase:wgEci99!
Generating key (this may take several minutes)...Key generation complete.

(When selecting a passphrase, keep in mind that good passphrases typically
have upper and lower case letters, digits and punctuation marks, and are
at least 8 characters in length.)

Enter the local keyfile passphrase: gtS!i-00
Verify the local keyfile passphrase:gtS!i-00
Generating key (this may take several minutes)...Key generation complete.

-----------------------------------------------
Generating Tripwire configuration file...

-----------------------------------------------
Creating signed configuration file...
Please enter your site passphrase: wgEci99!
Wrote configuration file: /usr/TSS/bin/tw.cfg

A clear-text version of the Tripwire configuration file
/usr/TSS/bin/twcfg.txt
has been preserved for your inspection.  It is recommended
```

```
that you delete this file manually after you have examined it.


-----------------------------------------------
Customizing default policy file...

-----------------------------------------------
Creating signed policy file...
Please enter your site passphrase: wgEci99!
Wrote policy file: /usr/TSS/policy/tw.pol

A clear-text version of the Tripwire policy file
/usr/TSS/policy/twpol.txt
has been preserved for your inspection.  This implements
a minimal policy, intended only to test essential
Tripwire functionality.  You should edit the policy file
to describe your system, and then use twadmin to generate
a new signed copy of the Tripwire policy.


-----------------------------------------------
The installation succeeded.

Please refer to /usr/TSS/Release_Notes
for release information and to the printed user documentation
for further instructions on using Tripwire 2.2.1 for Unix.
```

Configuring Tripwire

Configuring Tripwire depends on various parameters specific to your site. Please consult the provided *Tripwire User's Guide.* A quick reference card is also provided. See:

```
/usr/sgi/ise/tripwire/tripwire-2.2.1.pdf
/usr/sgi/ise/tripwire/tripwire-quick-reference-2.2.1.pdf
```

Suggestions for Secure Server Operations

This chapter contains the following:

Important Security Concepts

Perhaps the most important security concepts in operating an Internet service are the following:

- Every piece of software may contain bugs that can potentially be exploited by a malicious or mischievous user out on the Internet to gain some level of unauthorized control over server resources.
- It is probable that an Internet service will at some point come under some form of attack from one or more client systems on the Internet.
- A hacker only has to be lucky once. As the system administrator defending the server against attack, you have to be lucky every day. At some point, your luck may run out.

Given the existence of hackers on the Internet, it is unfortunately necessary to adopt a comprehensive security culture that includes the following key components:

- A siege mentality tempered by the need to deliver your service to legitimate users at an acceptable cost.
- A set of applications that repel documented modes of attack. New modes are continually being discovered and defensive countermeasures published. You need to keep current on the subject matter.
- A set of security policies and associated business processes that ensure the security applications are not undermined accidentally or for the sake of operator convenience.

Security White Paper

SGI has written the *Server Security: An Overview White Paper*, which provides a high-level introduction to security and general instructions for the secure configuration and operations of a 24/7 production Internet service.

The white paper is intended to provide system administrators less familiar with the complex issue of computer security insight into the actions already performed during system lockdown and file integrity assessment setup. It will help you to scope your security requirements and to limit your exposure to many types of attacks aimed at compromising your system and/or network.

You can access the white paper from the following URL:

`http://www.sgi.com/solutions/broadband/sgi_internet.html`

Additional Sources of Security Information

You should also read the following documents and Web sites in order to be informed about security issues in general:

- Site Security Handbook:

  `http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2196.txt`

- Linux Administrator's Security Guide:

  `http://www.securityportal.com/lasg`

- SGI security page:

  `http://www.sgi.com/support/security`

- Internet Engineering Task Force (IETF) security working group page:

  `http://www.ietf.org/html.charters/wg-dir.html#Security_Area`

- Computer Emergency Response Team (CERT) page:

  `http://www.cert.org`

- Netscape security page:

  `http://www.netscape.com/eng/security`

- W3 security FAQ:

  `http://www.w3.org/Security/Faq`

- BUGTRAQ page:

  `http://www.securityfocus.com`

- Hacker sites:
  - `http://www.slashdot.com`
  - `http://www.rootshell.com`

Index

X