SLES Security Guide

Klaus Weidner <klaus@atsec.com>

December 4, 2003; v2.33

Contents

1 Introduction **6**
- 1.1 Purpose of this document . . . 6
- 1.2 How to use this document . . . 6
- 1.3 What is a CC compliant System? . . . 6
  - 1.3.1 Hardware requirements . . . 7
  - 1.3.2 Software requirements . . . 7
  - 1.3.3 Environmental requirements . . . 7
  - 1.3.4 Operational requirements . . . 7
- 1.4 Requirements for the system's environment . . . 7
- 1.5 Requirements for the system's users . . . 8
- 1.6 Overview of the system's security functions . . . 9
  - 1.6.1 Identification and Authentication . . . 9
  - 1.6.2 Audit . . . 9
  - 1.6.3 Discretionary Access Control . . . 9
  - 1.6.4 Object Reuse . . . 9
  - 1.6.5 Security Management and System Protection . . . 9
  - 1.6.6 Secure Communication . . . 9
- 1.7 Overview of security relevant events . . . 10

2 Installation **10**
- 2.1 Supported hardware . . . 10
- 2.2 Selection of install options and packages . . . 11
- 2.3 Installing required updates . . . 13
  - 2.3.1 Automated SP3 upgrade . . . 14
  - 2.3.2 YaST SP3 upgrade . . . 14
  - 2.3.3 Installing the audit subsystem . . . 14

3 Secure initial system configuration **15**
- 3.1 Automated configuration of the system . . . 15
- 3.2 Add and remove packages . . . 16
- 3.3 Disable services . . . 19
- 3.4 Remove setuid/setgid root settings from binaries . . . 19
- 3.5 Update permissions for 'su' . . . 21
- 3.6 Disable root login over the network . . . 21
- 3.7 Setting up SSH . . . 22
- 3.8 Setting up xinetd . . . 22
- 3.9 Setting up FTP . . . 23
- 3.10 Setting up Postfix . . . 23
- 3.11 Setting up the audit subsystem . . . 23
  - 3.11.1 Installing the packages needed for auditing . . . 24
  - 3.11.2 Installing the updated *audit.o* kernel module . . . 24
  - 3.11.3 Setting up the audit configuration files . . . 24
  - 3.11.4 Starting `auditd` at boot as a system service . . . 25
  - 3.11.5 Starting `auditd` in fail-secure mode from `init` (OPTIONAL) . . . 25
- 3.12 Introduction to Pluggable Authentication Module (PAM) configuration . . . 25
- 3.13 Required Pluggable Authentication Module (PAM) configuration . . . 26
  - 3.13.1 /etc/pam.d/chage . . . 27
  - 3.13.2 /etc/pam.d/chfn . . . 27
  - 3.13.3 /etc/pam.d/chsh . . . 27
  - 3.13.4 /etc/pam.d/login . . . 28
  - 3.13.5 /etc/pam.d/other . . . 28
  - 3.13.6 /etc/pam.d/passwd . . . 28

3.13.7 /etc/pam.d/sshd . . . 29
3.13.8 /etc/pam.d/su . . . 29
3.13.9 /etc/pam.d/useradd . . . 29
3.13.10 /etc/pam.d/vsftpd . . . 30
3.13.11 /etc/security/pam_pwcheck.conf . . . 30
3.13.12 /etc/security/pam_unix2.conf . . . 30
3.14 Setting up login controls . . . 30
3.14.1 Maintaining *cracklib* dictionaries . . . 31
3.15 Configuring the boot loader . . . 31
3.15.1 GRUB boot loader configuration . . . 32
3.15.2 Yaboot boot loader configuration . . . 32
3.15.3 ZIPL boot loader configuration . . . 33
3.15.4 iSeries kernel slots . . . 33
3.16 Reboot and initial network connection . . . 33

4 System operation **34**
4.1 System startup, shutdown and crash recovery . . . 34
4.2 Backup and restore . . . 34
4.3 Gaining superuser access . . . 35
4.4 Installation of additional software . . . 35
4.5 Scheduling processes using `cron` and `at` . . . 36
4.6 Mounting filesystems . . . 37
4.7 Managing user accounts . . . 38
4.8 SYSV shared memory and IPC objects . . . 39
4.9 Configuring secure network connections with *stunnel* . . . 39
4.9.1 Introduction . . . 39
4.9.2 Creating an externally signed certificate . . . 40
4.9.3 Creating a self-signed certificate . . . 42
4.9.4 Activating the tunnel . . . 43
4.9.5 Using the tunnel . . . 43
4.9.6 Example 1: system status view . . . 43
4.9.7 Example 2: Using outbound encryption with a non-encrypting client . . . 44
4.9.8 Example 3: Secure SMTP delivery . . . 44
4.10 The Abstract Machine Testing Utility (AMTU) . . . 44

5 Monitoring, Logging & Audit **45**
5.1 Reviewing the system configuration . . . 45
5.2 System logging and accounting . . . 46
5.3 Configuring the audit subsystem . . . 46
5.3.1 Intended usage of the audit subsystem . . . 47
5.3.2 Selecting the events to be audited . . . 47
5.3.3 Reading and searching the audit records . . . 47
5.3.4 Starting and stopping the audit subsystem . . . 48
5.3.5 Storage of audit records . . . 49
5.3.6 Reliability of audit data . . . 49
5.4 System configuration variables in */etc/sysconfig* . . . 49
5.4.1 *suseconfig* . . . 49
5.4.2 *security* . . . 50
5.4.3 *cron* . . . 50
5.4.4 *language* . . . 50
5.4.5 *backup* . . . 50
5.4.6 *boot* . . . 50
5.4.7 *displaymanager* . . . 50
5.4.8 *kernel* . . . 50

5.4.9 *clock* . . . 50
5.4.10 *proxy* . . . 51
5.4.11 *windowmanager* . . . 51
5.4.12 *sysctl* . . . 51
5.4.13 *java* . . . 51
5.4.14 *mail* . . . 51
5.4.15 *hardware* . . . 51
5.4.16 *printer* . . . 51
5.4.17 *news* . . . 51
5.4.18 *console* . . . 51
5.4.19 *keyboard* . . . 52
5.4.20 *mouse* . . . 52
5.4.21 *lvm* . . . 52
5.4.22 *network* . . . 52
5.4.23 *syslog* . . . 52
5.4.24 *SuSEfirewall2* . . . 52
5.4.25 *hotplug* . . . 52
5.4.26 *ssh* . . . 52
5.4.27 *postfix* . . . 52
5.4.28 *bootloader* . . . 52
5.4.29 *audit* . . . 52

6 Security guidelines for users **53**
6.1 Online Documentation . . . 53
6.2 Authentication . . . 53
6.3 Password policy . . . 54
6.4 Access control for files and directories . . . 55
6.5 Data import / export . . . 56

7 Appendix **56**
7.1 Online Documentation . . . 56
7.2 Literature . . . 56
7.3 The script `/usr/lib/eal3/bin/sles-eal3` . . . 57
7.4 The file `/etc/permissions.eal3` . . . 64
7.5 The file `/etc/init.d/audit` . . . 80
7.6 The file `/etc/audit/audit.conf` . . . 83
7.7 The file `/etc/audit/filter.conf` . . . 84
7.8 The file `/etc/audit/eal3files.conf` . . . 94

1 Introduction

1.1 Purpose of this document

The SuSE Linux Enterprise Server (SLES) distribution is designed to provide a secure and reliable operating system for a variety of purposes. Because security requirements obviously depend on the applications and environment, it is not possible to simply certify that the system is ”secure” - a more precise definition is needed.

The Common Criteria (CC) provides a widely recognized methodology for security certifications. A CC evaluation is fundamentally a two-step process, consisting of defining the ”security target” which describes the features that are to be evaluated, and then testing and verifying that the system actually implements these features with a sufficient level of assurance.

This document is a security guide that explains how to set up the evaluated configuration, and provides information to administrators and ordinary users to ensure secure operation of the system. It is intended to be self-contained in addressing the most important issues at a high level, and refers to other existing documentation where more details are needed. The usual convention of referring to manual pages is used, i.e. *ls*(1) implies running the `man -S 1 ls` command (usually, `-S` and the section number may be omitted).

The document primarily addresses administrators, but the section ”Security guidelines for users” is intended for ordinary users of the system as well as administrators.

Knowledge of the Common Criteria is not required for readers of this document.

1.2 How to use this document

The key words ”MUST”, ”MUST NOT”, ”REQUIRED”, ”SHALL”, ”SHALL NOT”, ”SHOULD”, ”SHOULD NOT”, ”RECOMMENDED”, ”MAY”, and ”OPTIONAL” in this document are to be interpreted as described in RFC 2119 <http://www.ietf.org/rfc/rfc2119.txt>.

Note that the terms ”SHOULD” and ”SHOULD NOT” are avoided in this document. Requirements are either absolute (and marked with MUST and equivalent terms), or entirely optional (in the sense of not affecting required security functions) and marked with RECOMMENDED, MAY or OPTIONAL.

If you follow the requirements in this document when setting up and using the system, your configuration will match the evaluated configuration. Certain configuration options are marked as OPTIONAL and you MAY modify them as needed, but you MUST NOT do other changes, because they will make the system fail to match the evaluated configuration.

Of course, you MUST always use common sense. This document is not a formal specification, and legitimate reasons may exist to modify the system setup in ways not described here if that is necessary for the system to fulfill its intended purpose. Specifically, applying security patches released by the vendor is strongly RECOMMENDED even though that will cause a deviation from the evaluated configuration.

In cases where the requirements and recommendations in this document conflict with those in other sources (i.e. the online documentation), the information in this Security Guide has higher precedence. You MUST follow the steps described here to reach the evaluated configuration, even if other documentation describes different methods.

1.3 What is a CC compliant System?

A system can be considered to be ”CC compliant” if it matches an evaluated and certified configuration. This implies various requirements concerning hardware and software, as well as requirements concerning the operating environment and users and the ongoing operating procedures.

Strictly speaking, an evaluation according to the CC represents the results of investigation of the security properties of the target system according to defined guidelines. It should not be considered as a guarantee for fitness for any specific

purpose, but should provide help in deciding the suitability of the system considering how well the intended use fits the described capabilities, and will provide a level of assurance about the security functions that have been examined by a neutral third party.

1.3.1 Hardware requirements

The hardware MUST be the one of the following IBM system:

```
xSeries 335 (x86)

pSeries 630 (ppc 64-bit kernel)

iSeries 825 (ppc 64-bit kernel)

zSeries 900 (s390 31-bit kernel)

eServer 325 (x86_64 opteron)
```

Running the certified software on other similar hardware may result in an equivalent security level, but the certification does not apply if the hardware is different from that used for the testing processes during the evaluation.

1.3.2 Software requirements

The software MUST match the evaluated configuration. In the case of an operating system, this also requires that the installed kernel, system and application software are the same. The documentation (including this guide) will specify permitted variations, such as modifying certain configuration files and settings, and installing software that does not have the capability to affect the security of the system (typically those that do not require 'root' privileges).

1.3.3 Environmental requirements

Stated requirements concerning the operating environment MUST be met. Typical requirements include a secure location for the hardware (protected from physical access by unauthorized persons), as well as restrictions concerning permitted network connections.

1.3.4 Operational requirements

The operation of the system MUST be in agreement with defined organizational security policies, to ensure that actions by administrators and users do not undermine the system's security.

1.4 Requirements for the system's environment

The security target covers one or more systems running SLES, networked in a non-hostile network, with a well-managed and non-hostile user community. It is not intended to address the needs of an Internet-connected server, or the case where services are to be provided to potentially hostile users.

All network cabling MUST be secure and protected from tapping and other modifications. We require a secure network for the evaluated configuration because an examination of cryptographic protocols was beyond the evaluation's scope. Of course, the OpenSSH suite of tools are also in use in hostile environments, but this evaluation makes no assumptions about their security properties in such scenarios. Only the password authentication functionality offered by OpenSSH

is covered here, other authentication methods (such as public key authentication, Kerberos etc.) are not supported in the evaluated configuration.

You MUST set up the server (or servers) in a physically secure environment, where they are protected from theft and manipulation by unauthorized persons.

All components in the network such as routers, switches and hubs that are used for communication are assumed to pass the user data reliably and without modification. Translations on protocols elements (i.e. NAT) are allowed as long as those modifications do not lead to a situation where information is routed to somebody other than the intended recipient system.

Be aware that information passed to another system leaves the control of the sending system, and therefore the protection of this information against unauthorized access needs to be enforced by the receiving system. If an organization wants to implement a consistent security policy covering multiple systems on a network, organizational procedures MUST ensure that all those systems can be trusted and are configured with compatible security configurations enforcing an organization wide security policy. How to do this is beyond the scope of this Security Guide. If you set up a communication link to a system outside your control, please keep in mind that you will not able to enforce any security policy for any information you pass to such a system over the communication link or in other ways (i.e. by using removable storage media).

Every person that has the ability to perform administrative actions by switching to root has full control over the system and could either by accident or deliberately undermine the security of the system and bring it into an insecure state. This Security Guide provides the basic guidance how to set up and operate the system securely but is not intended to be the sole information required for a system administrator to learn how to operate Linux securely. It is assumed within this Security Guide that administrators who use this guide have a good knowledge and understanding of operating security principles in general and of Linux administrative commands and configuration options in particular. We strongly advise that an organization that wants to operate the system in the evaluated configuration nevertheless have their administrators trained in operating system security principles and SuSE Linux security functions, properties and configuration.

We also want to emphasize the fact that every organization needs to trust their system administrators not to deliberately undermine the security of the system. Although the evaluated configuration includes audit functions that can be used to make users accountable for their actions, we need to point out that an administrator is able to stop the audit subsystem and reconfigure it such that his actions no longer get audited. Well trained and trustworthy administrators are therefore a key element for the secure operation of the system. This Security Guide then provides the additional information a system administrator should obey when installing, configuring and operating the system in compliance with the requirements defined the Security Target for the Common Criteria evaluation.

1.5 Requirements for the system's users

The security target addresses the security needs of cooperating users in a benign environment, who will use the system responsibly to fulfill their tasks.

Note that system availability is *not* addressed in this evaluation, and a malicious user could disable a server through resource exhaustion or similar methods.

The requirements for users specifically include:

- User accounts MUST be assigned only to those users with a need to access the data protected by the system, and who MUST be sufficiently trustworthy not to abuse those privileges. For example, the system cannot prevent data from being intentionally redistributed to unauthorized third parties by an authorized user.
- All users of the system MUST be sufficiently skilled to understand the security implications of their actions, and MUST understand and follow the requirements listed in the section §6 "Security guidelines for users" of this document. Appropriate training MUST be available to ensure this.

It is part of your responsibility as a system administrator to verify that these requirements are met, and to be available to users if they need your help in maintaining the security of their data.

1.6 Overview of the system's security functions

This section summarizes the security functions that were covered by the evaluation. Please refer to the appropriate sections for information on configuring, using and managing these functions.

1.6.1 Identification and Authentication

Pluggable Authentication Module (PAM)

Sections §3.12 "Introduction to Pluggable Authentication Module (PAM) configuration", §3.13 "Required Pluggable Authentication Module (PAM) configuration"; the documentation in */usr/share/doc/packages/pam/* and the *pam*(8) man page.

login

Section §3.14 "Setting up login controls"; and the *login*(1) and *login.defs*(5) man pages.

OpenSSH

Section §3.7 "Setting up SSH" and the *sshd*(8), *ssh*(1), *sshd_config*(5) man pages.

vsftpd

Section §3.9 "Setting up FTP" and the *vsftpd*(8), *vsftpd.conf*(5) man pages.

su

Sections §3.5 "Update permissions for 'su'", §4.3 "Gaining superuser access"; and the *su*(8) man page.

1.6.2 Audit

Sections §3.11 "Setting up the audit subsystem" and §5.3 "Configuring the audit subsystem"; and the *laus*(7) man page, whose "SEE ALSO" section points to the remaining LAuS man pages.

1.6.3 Discretionary Access Control

Sections §6.4 "Access control for files and directories" and §4.8 "SYSV shared memory and IPC objects".

1.6.4 Object Reuse

See the SLES High Level Design document, the kernel automatically ensures that new objects (disk files, memory, IPC) do not contain any traces of previous contents.

1.6.5 Security Management and System Protection

Chapters §4 "System operation" and §5 "Monitoring, Logging & Audit".

1.6.6 Secure Communication

Section "Configuring secure network connections with *stunnel*" (§4.9) and the *stunnel*(1) man page.

Section §3.7 "Setting up SSH" and the *sshd*(8), *ssh*(1), *sshd_config*(5) man pages.

1.7 Overview of security relevant events

The audit subsystem is intended to be the central interface for collecting and viewing the record of security relevant events. The events being monitored by default in the evaluated configuration include:

- All authentication done through the PAM library, including the identity and location (where available) of the user and the success or failure result.
- Use of *su*(8) to change identity. All actions done as part of a *su* session are marked in the audit record with the original user's login user ID.
- Adding, changing or deleting users or groups.
- Changes and change attempts to the contents of security critical files.
- Changes to the access permissions or ownership of any files or IPC objects.
- Binding network ports and accepting connections.

Please refer to section §5 "Monitoring, Logging & Audit" for more information.

2 Installation

The evaluation covers a fresh installation of the SLES version 8 on one of the supported hardware platforms as defined in the section §1.3.1 "Hardware requirements" above.

On the platforms that support virtualization (VM) or secure logical partitioning (LPAR), other operating systems MAY be installed and active at the same time as the evaluated configuration if (and only if) the VM or LPAR configuration ensures that the other operating systems cannot access data belonging to the evaluated configuration or otherwise interfere with its operation. Setting up this type of configuration is considered to be part of the operating environment and is not addressed in this document.

On the other platforms, the evaluated configuration MUST be the only operating system installed on the server.

2.1 Supported hardware

You MAY attach the following peripherals without invalidating the evaluation results. Other hardware MUST NOT be installed in or attached to the system.

- Any storage devices and backup devices supported by the operating system (this includes hard disks, CD-ROM drives and tape drives).
- All Ethernet and Token Ring network adapters supported by the operating system. Modems, ISDN and other WAN adapters are not part of the evaluated environment.
- Any printers supported by the operating system.
- Operator console consisting of a keyboard, video monitor, and optionally mouse. Additionally, you may directly attach supported serial terminals, but *not* modems, ISDN cards or other remote access terminals.

Hot-pluggable hardware that depends on the dynamic loading of kernel modules is *not* supported. Examples of such unsupported hardware are USB, IEE1394/FireWire and PCMCIA/CardBus peripherals.

2.2 Selection of install options and packages

This section describes the detailed steps to be performed when installing the SLES operating system on the target server.

All settings listed here are REQUIRED unless specifically declared otherwise.

- Disconnect computer from all network connections. You MUST NOT reconnect them until the post-install configuration (including system hardening) is completed.
- Verify that the installation CD is an authentic SuSE distribution CD for SLES 8 with the label ”SuSE LINUX ENTERPRISE SERVER Installation” for your server’s architecture. The CD is shipped in a sealed sleeve.
- Launch the installer program contained on the CD-ROM. The details of how to do this depend on the hardware platform, please refer to the installation guide that is part of the printed manual accompanying the CD.

  For example:

  – xSeries, eServer: Insert the SLES 8 CD and boot from CD-ROM.
  – zSeries, pSeries: Details depend on the operation mode (VM, LPAR or native). The process generally involves copying the installer onto the server and launch the installer using the host’s management interface.
- Text mode MAY be chosen instead of the default graphical installation.

  You MAY also use a serial console to do a text-mode installation. To do so, connect a serial terminal (or a computer with terminal emulator software; such a computer MUST be appropriately secure) to the server’s serial port, and boot from the SLES CD. When the boot prompt is shown on the serial console, enter `install console=ttyS0` and press `ENTER` to start the installation.
- Accept the license agreement.
- Select your language: ”English (US)” (to ensure that the messages shown match those described in this guide).
- If prompted (due to having Linux installed already), choose ”New installation”.
- Installation settings:

  – Mode: ”New installation”
  – Keyboard layout: ”English (US)” MAY be changed
  – Mouse: OPTIONAL (not needed)
  – Partitioning:
    change ’/’ type to ”ext3”
    OPTIONAL: add other ext3 partitions, i.e. /var, /home
    OPTIONAL: modify swap space setting (MAY be disabled)
    For all ext3 partitions, choose ”Fstab Options” and set ”Arbitrary option value” to ”acl”. The additional options ”No access time” or ”Mount read-only” MAY be set as required.
  – Software: choose ”Minimum system” (or ”Minimum graphical system (without KDE)” if ”Minimum system” is not offered as an option), and confirm the choice. Extra packages will be removed during the following hardening steps.
  – Select ”Detailed selection” and add the following packages to the selection. This is easiest when ”Filter” is set to ”Search”, then you can enter (part of) the package names in the search field and add a check mark to the package in the search result.
    The packages marked as OPTIONAL are services that are part of the evaluated configuration but MAY be omitted if you do not need them for your system. Packages containing documentation files or viewers that this document refers to are marked as RECOMMENDED, but you MAY omit them.
    The installer will automatically choose an appropriate kernel (single processor or SMP) based on the detected hardware. You MAY override this choice and choose either the *k_deflt* or *k_smp* kernel package manually.

```
yast2-online-update       # OPTIONAL: Yast2 module: get security patches
                          # (only for use in local network, not Internet)
yast2-runlevel            # Yast2 module: manage program start/stop at boot
yast2-security            # Yast2 module: edit global security settings
yast2-sysconfig           # Yast2 module: edit contents of /etc/sysconfig/*
star                      # Data archival tool with ACL support
texinfo                   # RECOMMENDED: Info documentation viewer
man-pages                 # RECOMMENDED: Manual pages
howtoenh                  # RECOMMENDED: how-to documentation (HTML format)

sles-admin-x86+x86-64_en  # RECOMMENDED: Administrator Manual
sles-inst-x86+x86-64_en   # RECOMMENDED: Installation Manual
sles-admin-ipseries_en    #   (choose the manual set for your architecture)
sles-inst-ipseries_en     #
sles-admin-zseries_en     #
sles-inst-zseries_en      #

lprng                     # OPTIONAL: Print spooler
xinetd                    # OPTIONAL: XInetd (only used for vsftpd)
vsftpd                    # OPTIONAL: FTP daemon (needs xinetd)
stunnel                   # OPTIONAL: set up encrypted SSL tunnels
```

  - Booting: keep default (no other OS is permitted on the server).
  - Time zone:
    RECOMMENDED: keep hardware clock time as ”UTC”
    RECOMMENDED: set zone as appropriate for server location
  - Language: ”English (US)”

- Start installation: press ”Accept” and ”Yes, install” buttons.
- Installation will proceed. Insert the CDs as prompted by the installer.
- The installer will reboot to continue running on the installed system.
- Installer will switch to text mode, confirm the explanatory text about this.
- Password for ”root”, the administrator
  - choose according to the password policy (§6.3)
  - in ”Expert Options”, set Password Encryption: ”MD5”
- Add a new user
  - create account for one of the administrators (RECOMMENDED: whoever is doing the installation)
  - choose a username (not ’root’ or any other system account)
  - choose password according to the password policy (§6.3)
  - open the ”Details” dialog, and add membership in the additional group ”trusted” for this administrator. Close the dialog.
  - open ”Password settings” window and edit the settings according to the parameters described in the section §3.14 ”Setting up login controls”:

```
Issue warning how many days before password expiration?    5
How many days after password expires is the login usable? -1
Maximum number of days for the same password              60
Minimum number of days for the same password               1
```

The ”Expiration date” MAY be left blank. Close the dialog.

– press the ”Next” button to continue.

- Network cards configuration
  - Configure all installed network cards (zero or more) as appropriate for the platform. In the case of virtual network cards on zSeries or iSeries, these options are not available. The following options MUST be used for non-virtual network cards:
  - Set a static IP address for each card (MUST NOT use DHCP)
  - Select the ”Host name and name server” dialog.
  - Disable the ”Change host name via DHCP” setting.
  - Disable the ”Update name servers via DHCP” setting.
  - RECOMMENDED: set the system’s host name.
  - OPTIONAL: configure DNS servers and DNS search lists
  - OPTIONAL: set default gateway and/or static routes.
  - Modems and ISDN adapters MUST NOT be present.
  - We RECOMMEND that you disconnect all network connections until the post-install system configuration is finished. You MAY use a network if required for the installation (for example, zSeries hosts are usually installed using NFS, because they do not have a CD drive). If you do use a network, you MUST ensure that this network is secure.

2.3 Installing required updates

The base system from CD is not yet configured to meed the requirements for the installation.

You need to perform the following steps (detailed below) to achieve the evaluated configuration:

- Apply the Service Pack 3 (SP3) patches.
- Replace the default PAM authentication library with the audit-enabled *pam-laus* version.
- Install the *certification-sles-eal3* RPM and run the *sles-eal3* script.
- Reboot.

SLES8 Service Pack 3 MUST be applied to the system. Since the evaluated configuration does not permit an Internet connection, you MUST use a separate machine to download the update and transfer the files to the target system, i.e. using a CD-R disk. You MAY make the files available to other SLES systems in the secure network and use the YAST2 online update mechanism to retrieve the files from this local mirror, but you MUST NOT connect the target system to the Internet.

The ISO images are available for download from the SuSE maintenance web at the URL http://sdb.suse.de/en/psdb/html/ . There are two ISO images for each supported architecture, the first one containing the binaries (REQUIRED for installation) and the second one the source code (OPTIONAL).

You MUST verify that the MD5 checksum of the file(s) you downloaded is correct:

```
# md5sum *.iso
722baf8d785a011503ec70e26045e91c  UnitedLinux-1.0-SP-3-i386-RC4-CD1.iso
eebe03e60bee38464603fc9c90d31cd0  UnitedLinux-1.0-SP-3-i386-RC4-CD2.iso
2dcf46e3a0e6f50836500645df194a32  UnitedLinux-1.0-SP-3-x86-64-RC4-CD1.iso
88bf8cc4b5c736b9c7d670a1926b363f  UnitedLinux-1.0-SP-3-x86-64-RC4-CD2.iso
```

```
097b72f8cc8cb3e7f1cd9b2885b3d105  SLES-8-SP-3-ppc-RC4-CD1.iso
678cee58643537d58b461c1df2748be5  SLES-8-SP-3-ppc-RC4-CD2.iso
704330ee0987be127ea6c9f514a93d71  SLES-8-SP3-s390-RC4-CD1.iso
4c7ecd93cbb765a82eeeafe18fc8b090  SLES-8-SP3-s390-RC4-CD2.iso
```

Then, either burn the CD1 image to a CD-R, or alternatively use a loopback mount on the target system if you have copied the ISO file using some other method.

The mount point used MUST be */media/cdrom*, otherwise the upgrade will not work correctly:

```
# CD-ROM in default drive:
mount /media/cdrom

# Loopback mount of the image file (this example is for x86):
mount -o loop UnitedLinux-1.0-SP-3-i386-RC4-CD1.iso /media/cdrom
```

2.3.1 Automated SP3 upgrade

This RECOMMENDED method is fully automated, but the script is not available for all architectures.

```
# Run the non-interactive script:
/media/cdrom/install_update_rpms.sh
```

2.3.2 YaST SP3 upgrade

If you do not use the automated upgrade, you MUST do the SP3 upgrade through the YaST GUI:

- Mount the ISO image as described above.
- Launch `yast` from the shell prompt.
- Select the *Software* category, item *Patch CD Update*.
- Under *Choice of installation source*, choose *Expert*, and then choose *Directory*.
- In the *Local directory* dialog box, enter `/media/cdrom`.
- Choose *Next*.
- Select all available patches.
- Choose *OK* to install the patches, then *Finish* when it is done.

2.3.3 Installing the audit subsystem

You MUST also install the Linux Auditing Subsystem (LAuS) RPM package and the LAuS-enabled PAM library that are distributed on the SP3 CD-ROM.

Install the LAuS userspace tools (auditd etc.). On pSeries and iSeries, you need to install **both** the 64bit and the 32bit versions of the library. On all other platforms, the plain *laus* package is either the 32bit or 64bit version as required for the architecture.

```
# separate 64bit version on pSeries and iSeries only:
rpm -Uvh /media/cdrom/*/*/laus-64bit-0.1*.rpm
# all platforms (including pSeries and iSeries):
rpm -Uvh /media/cdrom/*/*/laus-0.1*.rpm
```

The LAuS-enabled PAM library is a drop-in replacement for the currently installed PAM library. PAM is a critical system component where an install error will result in an unusable system, you MUST use the following procedure:

```
# Install the replacement pam-laus library, overwriting files
# belonging to the original PAM library:
rpm -Uvh --force /media/cdrom/*/*/pam-laus-0.76*.rpm

# RECOMMENDED: verify that the installation was successful
# by logging in locally:
ssh localhost
```

The RPM database will still list the original *pam* package as being installed, even though all of its files were overwritten by the *pam-laus* package. This is necessary to keep dependencies satisfied, i.e. for the *pam-modules* package. You MUST NOT reinstall or update the *pam* package.

3 Secure initial system configuration

After the initial installation, the operating system is not yet in the evaluated configuration. The instructions in this section explain how to achieve that configuration.

After software upgrades or installation of additional packages, these steps MUST be re-done or at least re-checked to ensure that the configuration remains secure.

Log in as user 'root' on the system console for these steps.

3.1 Automated configuration of the system

The *certification-sles-eal3.rpm* package MUST be installed initially to achieve the evaluated configuration. This RPM package contains updates to the manuals, EAL3 specific configuration files and scripts to set up the evaluated configuration.

Please check the file */usr/share/doc/packages/certification-sles-eal3/README-eal3.txt* from the *certification-sles-eal3.rpm* for the latest errata information.

The certification-sles-eal3.rpm package contains a setup script that has to be run to implement the evaluated configuration: */usr/lib/eal3/bin/sles-eal3*.

The *certification-sles-eal3* RPM contains the following EAL3 specific configuration files:

```
/etc/permissions.eal3
```

We RECOMMEND that you use the `sles-eal3` script to reset the configuration to its initial state after any updates, but you MAY also perform the steps listed here manually.

WARNING: The `sles-eal3` script will reboot the system as the final step in the process, as described in the manual instructions in section §3.16 "Reboot and initial network connection". On zSeries, it will run the *zipl* boot configuration tool (with no arguments) before rebooting.

If you use the script, the remaining steps in this chapter are done automatically; skip ahead to the "System operation" chapter (§4).

3.2 Add and remove packages

The evaluated configuration REQUIRES the Abstract Machine Testing Utility to be present on the machine. This tool is provided in the *amtu* RPM package contained within the *certification-sles-eal3* RPM in the directory */usr/lib/eal3/rpm/*. It will be installed automatically by the `sles-eal3` script.

The minimal install still contains some packages that MUST be removed for the evaluated configuration. Use `rpmqpack` to get a list of installed packages, and `rpm -e PACKAGE_NAME ...` to remove all packages EXCEPT those listed here.

Some packages are listed as RECOMMENDED or OPTIONAL in section §2.2 ”Selection of install options and packages”. If you did not select all of those, some of the following packages will not be present on your system.

The evaluated configuration including all RECOMMENDED and OPTIONAL packages consists of exactly the following packages:

```
all architectures:
    UnitedLinux-build-key     openldap2-client
    aaa_base                  openssh
    aaa_skel                  openssl
    acl                       pam-laus
    amtu                      pam-modules
    ash                       parted
    at                        pciutils
    attr                      pcre
    bash                      perl
    bc                        permissions
    bzip2                     popt
    certification-sles-eal3   postfix
    cpio                      ps
    cracklib                  readline
    cron                      rpm
    curl                      sed
    cyrus-sasl                sh-utils
    db                        shadow
    devs                      sitar
    dialog                    sles-release
    diffutils                 star
    e2fsprogs                 stunnel
    ed                        suse-build-key
    file                      sysconfig
    filesystem                syslogd
    fileutils                 sysvinit
    fillup                    tar
    findutils                 telnet
    gawk                      terminfo
    gdbm                      texinfo
    glibc                     textutils
    gpg                       timezone
    gpm                       utempter
    grep                      util-linux
    groff                     vim
    gzip                      vsftpd
    hdparm                    w3m
    heimdal-lib               wget
```

```
    howtoenh                  xinetd
    hwinfo                    yast2
    iproute2                  yast2-bootloader
    iputils                   yast2-core
    ksymoops                  yast2-country
    l2h-pngicons              yast2-installation
    laus                      yast2-mouse
    less                      yast2-ncurses
    libgcc                    yast2-network
    libstdc++                 yast2-online-update
    libxcrypt                 yast2-packagemanager
    libxml2                   yast2-packager
    liby2util                 yast2-pam
    logrotate                 yast2-runlevel
    lprng                     yast2-security
    lukemftp                  yast2-storage
    m4                        yast2-sysconfig
    mailx                     yast2-theme-SuSELinux
    man                       yast2-trans-en_US
    man-pages                 yast2-transfer
    mktemp                    yast2-update
    modutils                  yast2-users
    ncurses                   yast2-xml
    net-tools                 zlib
    netcat
    netcfg

additional on x86 (xSeries):
    either the "k_deflt" or the "k_smp" kernel
    freetype2
    grub
    isapnp
    kbd
    sles-admin-x86+x86-64_en
    sles-inst-x86+x86-64_en
    unitedlinux-release
    yast2-theme-UnitedLinux

additional on x86_64 (eServer 325 (opteron))
    either the "k_deflt" or the "k_smp" kernel
    freetype2
    grub
    glibc-32bit
    isapnp
    kbd
    sles-admin-x86+x86-64_en
    sles-inst-x86+x86-64_en
    unitedlinux-release
    yast2-theme-UnitedLinux

additional on ppc (pSeries):
    addonlibs-64bit
    baselibs-64bit
```

```
    glibc-64bit
    hfsutils
    isapnp
    kbd
    kernel-ppc64
    laus-64bit
    lilo
    pdisk
    sles-admin-ipseries_en
    sles-inst-ipseries_en

additional on ppc (iSeries):
    addonlibs-64bit
    baselibs-64bit
    freetype2
    glibc-64bit
    hfsutils
    isapnp
    kernel-iseries64
    kernel-iseries64-tools
    laus-64bit
    lilo
    pdisk
    sles-admin-ipseries_en
    sles-inst-ipseries_en

additional on s390 (zSeries):
    freetype2
    glibc-locale
    k_deflt
    s390-tools
    sles-admin-zseries_en
    sles-inst-zseries_en
```

The *pam* package will be listed in the RPM database as being installed, but all of its files were overwritten by the *pam-laus* package. You MUST NOT try to uninstall, reinstall or update the *pam* package.

In addition to these packages, certain additional software from the SLES CDs MAY be installed without invalidating the evaluated configuration. The rules described in the section §4.4 ”Installation of additional software” MUST be followed to ensure that the security requirements are not violated.

The following packages are examples of tolerated packages that MAY be added to the system according to these rules. Note that the software contained in these packages is not intended to be used with ’root’ privileges, but the presence of the packages does not invalidate the evaluated configuration. The `sles-eal3` script does not remove these packages if they are installed on the system:

```
    attr-devel                  perl-Convert-BER
    autoconf                    perl-Crypt-DES
    automake                    perl-DateManip
    binutils                    perl-Digest-HMAC
    cpp                         perl-Digest-SHA1
    cross-ppc64-binutils        perl-Expect
    cross-ppc64-gcc             perl-HTML-Parser
    cross-ppc64-glibc           perl-HTML-Tagset
```

```
cross-ppc64-libs_and_headers  perl-IO-Stty
cvs                           perl-IO-Tty
expect                        perl-Mon
flex                          perl-Net-SNMP
gcc                           perl-Net_SSLeay
gcc-c++                       perl-Tie-IxHash
gettext                       perl-Time-Period
glib                          perl-TimeDate
glibc-devel                   perl-Tk
glibc-locale                  perl-URI
kernel-source                 perl-gettext
laus-devel                    perl-libwww-perl
libgcc                        strace
libstdc++-devel               tcl
make                          tk
openssl-devel                 xshared
pam-devel
patch
```

3.3 Disable services

Note: The system runlevel as specified in the 'initdefault' entry in */etc/inittab* MUST remain at the default setting of '3' for these steps to be valid.

Only the following services are allowed for runlevel 3:

```
atd
audit
cron
hwscan
kbd
lpd
network
postfix
random
rpmconfigcheck
sshd
syslog
xinetd
```

All others MUST be removed with *insserv -r ServiceName*.

Make sure that the audit subsystem is activated and the startup symlink */etc/init.d/rc3.d/S01audit* exists and points to */etc/init.d/audit*. If `auditd` is not running, all logins are automatically disabled as required by CAPP. If it is missing, create the link with *insserv audit*.

3.4 Remove setuid/setgid root settings from binaries

Use of the setuid bit on binaries (to run with root privileges) MUST be limited to those shown in the following list. The other binaries that were installed "setuid root" MUST have this bit removed. 'root' can still run these binaries normally, but they are not available for ordinary users.

```
/bin/ping
/bin/su
/usr/bin/at
/usr/bin/chage
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/crontab
/usr/bin/gpasswd
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/lpstat
/usr/bin/passwd
```

There is also a number of SGID files on the system that are needed:

```
/usr/sbin/postdrop    # group "maildrop"
/usr/sbin/postqueue   # group "maildrop"
/usr/sbin/utempter    # group "tty"
```

For informational purposes, here is a non authorative list of programs that have their setuid or setgid bit removed:

```
/bin/mount
/bin/ping6
/bin/umount
/sbin/unix2_chkpwd
/sbin/unix_chkpwd
/usr/bin/expiry
/usr/bin/mandb
/usr/bin/newgrp
/usr/bin/ssh
/usr/bin/wall
/usr/bin/write
/usr/lib/pt_chown
/usr/sbin/lpc
```

Similarly, the setgid bit MUST NOT be used to give group ”root” privileges to any binary.

The SuSE permission mechanism MUST be used to set permission bits appropriately. First make sure that no SUID/SGID programs are present on the system:

```
find / \( ! -fstype ext3 -prune -false \) -o  \
   -type f \( -perm -4000 -o -perm -2000 \) \
   -exec chmod u-s,g-s {} \; -print
```

Make sure that */etc/sysconfig/security* has the following two variables set:

```
CHECK_PERMISSIONS=set
PERMISSION_SECURITY="eal3"
```

Then run `chkstat -set /etc/permissions.eal3` to set the needed SUID and SGID bits.

3.5 Update permissions for 'su'

The 'su' binary MUST be restricted to members of the 'trusted' group. This will be enforced both with PAM configuration (configured later) and the binary's permissions.

```
chgrp trusted /bin/su
chmod 4710 /bin/su
```

When running the *chkstat* command as described above, this will be configured automatically.

3.6 Disable root login over the network

Login from the network with user ID 0 ('root') MUST NOT be permitted over the network. Administrators MUST use an ordinary user ID to log in, and then use the `/bin/su -` command to switch identities. For more information, refer to the section §4.3 "Gaining superuser access" below.

We RECOMMENDED that you remind administrators of this by adding the following alias to the bash configuration file */etc/bash.bashrc.local* that disables the pathless 'su' command:

```
alias su="echo \"Always use '/bin/su -' (see Security Guide)\""
```

This alias can be disabled for the root user in */root/.bashrc*:

```
unalias su
```

The restriction for direct root logins is enforced through two separate mechanisms. For network logins using ssh, the `PermitRootLogin no` entry in */etc/ssh/sshd_config* MUST be set (see next section). Console and serial terminal logins use the `pam_securetty.so` PAM module in the */etc/pam.d/login* file, which verifies that the terminal character device used is listed in the file */etc/securetty*.

The file */etc/securetty* MUST NOT be changed from the secure default settings as originally installed:

```
#
# This file contains the device names of tty lines (one per line,
# without leading /dev/) on which root is allowed to login.
#
tty1
tty2
tty3
tty4
tty5
tty6
# for devfs:
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
```

3.7 Setting up SSH

SSH protocol version 1 MUST be disabled. It has known security deficiencies.

The ssh client MUST NOT be set up setuid root (the setuid bit was removed in the post-install configuration). This prevents the use of some authentication methods normally supported by OpenSSH, but does not affect the evaluated configuration which uses password authentication exclusively.

The SSH Server MUST be configured to reject attempts to log in as root.

The permitted authentication mechanisms are per-user (nonempty) passwords and per-user DSS public key authentication. All other authentication methods MUST be disabled.

The setting `PAMAuthenticationViaKbdInt` MUST be disabled, since this would otherwise circumvent the disabled root logins over the network.

This results in the following option set for the SSH daemon that MUST be set in /etc/ssh/sshd_config:

```
Protocol 2
Ciphers 3des-cbc
PermitRootLogin no
RSAAuthentication no
PubkeyAuthentication yes
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no
PasswordAuthentication yes
PermitEmptyPasswords no
ChallengeResponseAuthentication no
KerberosAuthentication no
GSSAPIAuthentication no
PAMAuthenticationViaKbdInt no
X11Forwarding no
Subsystem sftp /usr/lib/ssh/sftp-server
```

All other options MUST NOT be changed from the defaults or from those settings specified here. Specifically, you MUST NOT add other authentication methods (AFS, Kerberos, host-based) to those permitted here.

3.8 Setting up xinetd

The *xinetd* super server is used to start the FTP daemon. The defaults entry in the */etc/xinetd.conf* file specifies the log file and the data that is to be logged:

```
defaults
{
       log_type        = FILE /var/log/xinetd.log
       log_on_success  = PID HOST EXIT DURATION
       log_on_failure  = HOST ATTEMPT RECORD
       instances       = 2
}
```

Please see the man page for *xinetd.conf* for more information on *xinetd* and configuration examples.

3.9 Setting up FTP

The system includes FTP services. The FTP server is started via *xinetd*, see *xinetd*(8). The following entry is the only active configuration entry in */etc/xinetd.conf*:

```
service ftp
{
       socket_type     = stream
       protocol        = tcp
       wait            = no
       user            = root
       server          = /usr/sbin/vsftpd
       instances       = UNLIMITED
}
```

The *vsftpd* uses several additional configuration files. In */etc/vsftpd.conf* the configuration of the ftp daemon is specified. In addition, for access control, the classic */etc/ftpusers* file is used. Users listed in the *ftpusers* file can NOT log in via FTP. This file initially contains all system IDs and the root user. It can be augmented with other IDs according to the local needs. The *ftpusers* file in not checked by the ftp daemon itself but by a PAM module. Please see the section §**??** "Required PAM configuration" for details.

The setup of */etc/vsftpd.conf* depends on the local needs. Please refer to *vsftpd.conf*(5) for details.

The default configuration permits only anonymous FTP. This setting is therefore only suitable for distribution of public files for which no read access control is needed. We RECOMMEND disabling anonymous FTP if you do not need this functionality with the following setting in */etc/vsftpd.conf*:

```
anonymous_enable=NO
```

You MAY enable FTP authentication for local user accounts. The corresponding setting in */etc/vsftpd.conf* is:

```
local_enable=YES
```

We RECOMMEND using *scp*(1) to copy files among users, and to use FTP only for legacy applications that do not support this alternative.

3.10 Setting up Postfix

The default settings of the postfix MTA are in accordance with the EAL3 requirements. An alias MUST be set up for root in */etc/aliases*, as postfix will not deliver mail while running with UID 0. Specify one or more user names of administrators to whom mail addressed to *root* will be forwarded.

Please see *postfix*(1), *master*(8) and the documentation in */usr/share/doc/packages/postfix/html/* for details.

3.11 Setting up the audit subsystem

This section describes only the initial setup and default configuration of the audit subsystem. Please refer to the section §5.3 "Configuring the audit subsystem" below for information about how it works and what changes MAY be made to the configuration.

3.11.1 Installing the packages needed for auditing

The required packages have already been installed in the previous step described in section §2.3 ”Installing required updates”. The audit subsystem consists of the following packages:

kernel-source, k_deflt, k_smp

The kernels include the audit modifications, including the driver *drivers/audit/** and the required hooks in the rest of the kernel.

laus

Contains the userspace Linux Auditing Subsystem (LAuS) programs including *auditd*(8), *aucat*(8) and *augrep*(8), the *liblaus.so* shared library, the */etc/init.d/audit* startup script, the configuration in */etc/sysconfig/audit*, the `/lib/security/pam_laus.so` PAM module and the corresponding man pages. The corresponding development libraries and headers are in the *laus-devel* RPM which is not installed as part of the evaluated configuration.

pam-laus

Contains an enhanced version of the PAM framework library that replaces the package *pam*. This library is a drop-in replacement that does not change the behavior of PAM, but generates an audit record for each use of a module stack.

at, cron, shadow

These packages contain audit-enabled versions of the trusted programs, which will generate audit records for security relevant events.

This section describes the further changes that need to be made to reach the initial state of the evaluated configuration.

3.11.2 Installing the updated *audit.o* kernel module

The audit module distributed as part of the SLES8-SP3 kernel packages MUST be replaced with the updated copy contained within the *certification-sles-eal3* RPM package, in the subdirectory of */usr/lib/eal3/lib/kernel/* matching the current architecture. This is done automatically by the `sles-eal3` script.

If you manually rebuild the kernel and/or modules, you MUST ensure that the corresponding patch in */usr/lib/eal3/lib/kernel/* is applied to the kernel source.

3.11.3 Setting up the audit configuration files

Use the following settings in the file */etc/sysconfig/audit*:

```
AUDIT_ALLOW_SUSPEND=1
AUDIT_ATTACH_ALL=0
AUDIT_MAX_MESSAGES=1024
AUDIT_PARANOIA=0
```

In addition, set up the following files with the content shown in the corresponding appendix of this document:

```
/etc/init.d/audit
/etc/audit/audit.conf
/etc/audit/filter.conf
/etc/audit/eal3files.conf
```

The `sles-eal3` script automatically sets up this configuration.

3.11.4 Starting `auditd` at boot as a system service

The evaluated configuration runs `auditd` as a standard daemon service launched as part of the normal startup sequence, this is activated with the following command:

```
insserv audit
```

3.11.5 Starting `auditd` in fail-secure mode from `init` (OPTIONAL)

Running `auditd` as a system service is the standard and recommended method, other system components such as `cron` and `atd` are also launched in this way.

However, if `auditd` is killed or unexpectedly terminates, audit messages will be lost until the administrator restarts the service. This failure mode does not violate CAPP requirements, because only the sysadmin can kill the audit daemon, and the only failure mode addressed by CAPP concerns running out of disk space which is handled directly by `auditd`. Any other abnormal termination would indicate a serious bug that should be investigated, reported and fixed.

If you want to ensure that an instance of `auditd` will always be running even in case of these unusual failure modes, you MAY set up an alternative configuration and launch `auditd` via the `init` daemon.

To do this, disable the *audit* system service and instead create and activate an entry in the file */etc/inittab*:

```
insserv -r audit
echo "au:35:/etc/init.d/audit inittab" >> /etc/inittab
init q
```

This operating mode ensures that an instance of `auditd` will always be running, because `init` will automatically restart `auditd` immediately if it terminates for any reason. If `init` cannot restart `auditd` in this way, it will generate a *syslog* warning message and deactivate the *inittab* entry for five minutes, then try again.

3.12 Introduction to Pluggable Authentication Module (PAM) configuration

The PAM subsystem is responsible for maintaining passwords and other authentication data. Because this is a security-critical system, understanding how it works is very important. In addition to the *pam*(8) manual page, full documentation is available in */usr/share/doc/packages/pam/text/*, and includes *"The Linux-PAM System Administrator's Guide"* (*pam.txt*) as well as information for writing PAM applications and modules. Detailed information about modules is available in */usr/share/doc/packages/pam/modules/README.pam_**, as well as manual pages for individual modules, i.e. *pam_pwcheck*(8).

The PAM configuration is stored in the */etc/pam.d/* directory. Note that the documentation refers to a file */etc/pam.conf* which is not used by SLES (PAM was compiled to ignore this file if the */etc/pam.d/* directory exists).

Each service (application) that uses PAM for authentication uses a *service-name* to determine its configuration, stored in the file */etc/pam.d/SERVICE_NAME*. The special *service-name* **OTHER** (case insensitive) is used for default settings if there are no specific settings.

The configuration file for the service contains one entry for each module, in the format:

```
module-type   control-flag   module-path   args
```

Comments MAY be used, extending from '#' to the end of the line, and entries MAY be split over multiple lines, using a backslash at the end of a line as a continuation character.

The *module-type* defines the type of action being done. This can be one of four types:

auth

Authenticates users (determines that they are who they claim to be). It can also assign credentials, i.e. additional group memberships beyond those specified through */etc/passwd* and */etc/groups* - this additional functionality MUST NOT be used.

account

Account management not related to authentication, i.e. restricting access based on time of day, available system resources or the location of the user (network address or system console).

session

Manages resources associated with a service by running specified code at the start and end of the session. Typical usage includes logging and accounting, and initialization such as auto mounting a home directory.

password

Used for updating the password (or other authentication token), i.e. when using the *passwd*(1) utility to change it.

The *control-flag* specifies the action that will be taken based on the success or failure of an individual module. The modules are stacked (executed in sequence), and the *control-flags* determine which final result (success or failure) will be returned, thereby specifying the relative importance of the modules.

Stacked modules are executed in the order specified in the configuration file.

The *control-flag* can be specified as either a single keyword, or alternatively with a more elaborate syntax that allows greater control. SLES uses only the single keyword syntax by default.

required

If this module returns a failure code, the entire stack will return failure. The failure will be reported to the application or user only after all other modules in the stack have been run, to prevent leakage of information (for example, ask for a password even if the entered username is not valid).

requisite

Same as **required**, but return failure immediately, not executing the other modules in the stack. Can be used to prevent a user from entering a password over an insecure connection.

sufficient

Return success immediately if no previous **required** modules in the stack have returned failure. Do not execute succeeding modules.

optional

The return code of this module is ignored, except if all other modules in the stack return an indeterminate result (PAM_IGNORE).

The *module-path* specifies the filename of the module to be run (relative to the directory */lib/security/*, and the optional *args* are passed to the module - refer to the module's documentation for supported options.

3.13 Required Pluggable Authentication Module (PAM) configuration

You MUST restrict authentication to services that are explicitly specified. The 'other' fallback MUST be disabled by specifying the *pam_deny.so* module for each *module-type* in the 'other' configuration. This ensures that access decisions within the PAM system are handled only by the service specific PAM configuration.

You MUST add the *pam_wheel.so* module to the 'auth' *module_type* configuration for the 'su' service and specify the 'trusted' group.

You MUST add the *pam_tally.so* module to the 'auth' *module_type* configuration to disable accounts after a certain number of failed login attempts. Be aware that this can be used in denial-of-service attacks to lock out legitimate users.

You MUST use the *pam_passwdqc.so* password quality checking module to ensure that users will not use easily-guessable passwords.

You MUST NOT modify other settings, specifically you MUST use the 'md5' and 'use_cracklib' options for the *pam_pwcheck.so* module.

The 'remember=XX' option must be added to the */etc/security/pam_pwcheck.conf* file to force users to create new passwords and not re-use ones that they had previously, i.e. to prevent users from simply alternating between two passwords when asked to change it due to expiration. XX is any number between 7 and 400.

The system supports many other PAM modules apart from the ones shown here. In general, PAM modules that restrict logins further MAY be used. You MUST NOT weaken the login restrictions through configuration changes of the modules shown here or via additional modules.

Here are are the pam configuration files:

3.13.1 /etc/pam.d/chage

This file configures the access control for the *chage* command. It allows the use of chage only after the user's password has been entered or the calling user is 'root'.

```
#%PAM-1.0
# root is allowed to use chage without authentication
auth     sufficient    pam_rootok.so
auth     required      pam_unix2.so
account  required      pam_permit.so
password required      pam_deny.so
session  required      pam_deny.so
```

3.13.2 /etc/pam.d/chfn

This file configures the access control for the *chfn* command. It allows the use of chfn only after the user's password has been entered or the calling user is 'root'.

```
#%PAM-1.0
auth     sufficient     pam_rootok.so
auth     required       pam_unix2.so
account  required       pam_unix2.so
password required       pam_deny.so
session  required       pam_deny.so
```

3.13.3 /etc/pam.d/chsh

This file configures the access control for the *chsh* command. It allows the use of chsh only after the user's password has been entered or the calling user is 'root'.

```
#%PAM-1.0
auth     sufficient    pam_rootok.so
auth     required      pam_unix2.so
account  required      pam_unix2.so
password required      pam_deny.so
session  required      pam_deny.so
```

3.13.4 /etc/pam.d/login

This file configures the behavior of the *login* program. It allows root login only for terminals configured in */etc/securetty*. If the file */etc/nologin* is present, then only root can log in. The optional *pam_env* module MAY be used to set environment variables from */etc/security/pam_env.conf*. The optional pam_mail module MAY be used to notify the user that there is new mail. The *pam_tally* module MUST be used to block the user after 5 failed login attempts. The optional *pam_limits* module MAY be used to enforce resource limits via */etc/security/limits.conf*.

```
#%PAM-1.0
auth     required      pam_tally.so onerr=fail no_magic_root
auth     requisite     pam_unix2.so
auth     required      pam_securetty.so
auth     required      pam_nologin.so
auth     required      pam_env.so      # optional
auth     required      pam_mail.so     # optional
account  required      pam_unix2.so
account  required      pam_tally.so deny=6 reset no_magic_root
password requisite     pam_passwdqc.so ask_oldauthtok=update check_oldauthtok
password requisite     pam_pwcheck.so  use_first_pass use_authtok
password required      pam_unix2.so    use_first_pass use_authtok
session  required      pam_unix2.so
session  required      pam_limits.so   # optional
session  optional      pam_laus.so     # no lockout on failure
```

3.13.5 /etc/pam.d/other

This configuration applies for all PAM usage for which no explicit service is configured. It will log and block any attempts.

```
#%PAM-1.0
auth     required      pam_warn.so
auth     required      pam_deny.so
account  required      pam_warn.so
account  required      pam_deny.so
password required      pam_warn.so
password required      pam_deny.so
session  required      pam_warn.so
session  required      pam_deny.so
```

3.13.6 /etc/pam.d/passwd

This service configuration applies to password changes. Please see also */etc/security/pam_pwcheck.conf*.

```
#%PAM-1.0
auth     required      pam_unix2.so
account  required      pam_unix2.so
password requisite     pam_passwdqc.so ask_oldauthtok=update check_oldauthtok
password requisite     pam_pwcheck.so  use_first_pass use_authtok
password required      pam_unix2.so    use_first_pass use_authtok
session  required      pam_unix2.so
```

3.13.7 /etc/pam.d/sshd

This file configures the PAM usage for SSH. This is identical to the *login* configuration except for the *securetty* entry which is not applicable to network logins.

```
#%PAM-1.0
auth     required      pam_tally.so onerr=fail no_magic_root
auth     required      pam_unix2.so
auth     required      pam_nologin.so
auth     required      pam_env.so      # optional
account  required      pam_unix2.so
account  required      pam_nologin.so
account  required      pam_tally.so deny=6 reset no_magic_root
account  required      pam_laus.so detach
password requisite     pam_passwdqc.so ask_oldauthtok=update check_oldauthtok
password requisite     pam_pwcheck.so  use_first_pass use_authtok
password required      pam_unix2.so    use_first_pass use_authtok
session  required      pam_unix2.so
session  required      pam_limits.so   # optional
```

3.13.8 /etc/pam.d/su

This file configures the behavior of the 'su' command. Only users in the trusted group can use it to become 'root', as configured with the *pam_wheel* module.

```
#%PAM-1.0
auth     sufficient     pam_rootok.so
auth     required       pam_wheel.so use_uid group=trusted
auth     required       pam_unix2.so
auth     required       pam_tally.so onerr=fail no_magic_root
account  required       pam_unix2.so
account  required       pam_tally.so no_magic_root # deny=5 reset
password required       pam_deny.so
session  required       pam_unix2.so
```

Forcing the root user to change the root password is not desired here, therefore the *pam_unix2.so* module is absent in the *password* branch and *pam_deny.so* is used instead.

3.13.9 /etc/pam.d/useradd

This file allows the root user to add accounts without entering the root password.

```
#%PAM-1.0
auth     sufficient    pam_rootok.so
auth     required      pam_deny.so
account  required      pam_permit.so
password required      pam_permit.so
session  required      pam_deny.so
```

3.13.10 /etc/pam.d/vsftpd

This file configures the authentication for the FTP daemon. With the listfile module, users listed in /etc/ftpusers are denied FTP access to the system.

```
#%PAM-1.0
auth     required       pam_tally.so onerr=fail no_magic_root
auth     required       pam_listfile.so item=user sense=deny \
                            file=/etc/ftpusers onerr=fail
auth     required       pam_unix2.so
account  required       pam_unix2.so
account  required       pam_tally.so deny=6 reset no_magic_root
account  required       pam_laus.so detach
password required       pam_deny.so
session  required       pam_unix2.so
```

Note that the FTP protocol has no provisions for changing passwords, therefore the *pam_unix2.so* module is absent in the *password* branch and *pam_deny.so* is used instead.

3.13.11 /etc/security/pam_pwcheck.conf

This file contains the default option for the *pam_pwcheck* module. This makes it easier to set a global policy. The *md5* option enables long passwords (up to 127 characters, see also the limit in */etc/login.defs*, and the *use_cracklib* option activates password quality checks against standard dictionary and permutation attacks. The *remember* option ensures that the user does not reuse passwords by keeping track of the specified number of previously used passwords in the file */etc/security/opasswd*.

```
password:   md5 use_cracklib remember=7
```

3.13.12 /etc/security/pam_unix2.conf

This file contains the default option for the *pam_unix2* module. This makes it easier to set a global policy. The *md5* option enables long passwords (up to 127 characters, see also the limit in */etc/login.defs*. The *trace* option activates session tracing (start/stop) via *syslog*.

```
auth:
account:
password:   md5
session:    trace
```

3.14 Setting up login controls

The system supports various options to control log ins in */etc/login.defs*. The following table explains the options and the values needed for the EAL3 system.

The UMASK entry sets the *default* umask to the most restrictive setting. Users and processes MAY override this setting as required, i.e. through a setting in their personal shell profile or a service-specific configuration file.

```
FAIL_DELAY          3         # Delay between failed logins
                              # in seconds (MUST be at least 3)
FAILLOG_ENAB        yes       # Enable logging of failed log ins
```

```
                                # (login program only)
LOG_UNKFAIL_ENAB     no         # Do not display unknown
                                # user names on failed log ins
LASTLOG_ENAB         yes        # Log last log in
OBSCURE_CHECKS_ENAB  yes        # Enable more strict password checks
UMASK                077        # Default File permission mask
PASS_MAX_DAYS        60         # Maximum password life time (<= 60)
PASS_MIN_DAYS        1          # Minimum password life time
                                # (0 < PASS_MIN_DAYS < PASS_MAX_DAYS)
PASS_MIN_LEN         8          # Minimum password length
                                # (MUST be at least 8)
PASS_WARN_AGE        5          # Warn days before expiry
CRACKLIB_DICTPATH    /usr/lib/cracklib_dict
                                # Base name of the cracklib library
LOGIN_RETRIES        3          # Retries before the login
                                # process is killed
LOGIN_TIMEOUT        60         # Max time in seconds per login attempt
PASS_CHANGE_TRIES    3          # Max attempts at changing passwords
PASS_ALWAYS_WARN     yes        # Warn even root about weak passwords
PASS_MAX_LEN         127        # Maximum usable length of password
CHFN_AUTH            yes        # Require password for chfsn/chsh
CHFN_RESTRICT        rwh        # Fields that chfn may change
DEFAULT_HOME         no         # Disallow login without home directory
```

3.14.1 Maintaining *cracklib* dictionaries

The dictionary files used by *cracklib* are stored in */usr/lib/*:

```
/usr/lib/cracklib_dict.hwm
/usr/lib/cracklib_dict.pwd
/usr/lib/cracklib_dict.pwi
```

To create custom dictionary files instead of the supplied ones, the command */usr/sbin/create-cracklib-dict* MAY be used as follows:

```
/usr/sbin/create-cracklib-dict wordlist wordlist ...
```

This will generate a new set of dictionary files from the supplied word lists. Suggested word lists are included in the source RPM package of *cracklib*. We RECOMMEND adding dictionaries for your local language and other languages likely to be known by your user community.

3.15 Configuring the boot loader

You MUST set up the server in a secure location where it is protected from unauthorized access, which is sufficient to protect the boot process.

We nevertheless RECOMMEND to configure the following additional protection mechanisms:

- Ensure that the installed system boots exclusively from the disk partition containing SLES, and not from floppy disks, USB drives, CD-ROMs or other devices.
- Ensure that this setting cannot be modified, i.e. by using a BootProm/BIOS password to protect access to the configuration.

3.15.1 GRUB boot loader configuration

The GRUB boot loader is used on the xSeries and eServer 350 (Opteron) platforms. It is highly configurable, and permits flexible modifications at boot time through a special-purpose command line interface. Please refer to the *grub*(8) man page or run `info grub` for more information.

- Use the `password` command in */boot/grub/menu.lst* to prevent unauthorized use of the boot loader interface. We RECOMMEND that you use md5 encoding, run the command 'grub-md5-crypt' to generate the encoded version of a password.
- Protect all menu entries other than the default SLES boot with the 'lock' command (add in a single line after 'title') to prompt for a password when booting from other media (i.e. floppy).
- Remove group and world read permissions from the grub configuration file if it contains a password:

  ```
  chmod 600 /boot/grub/menu.lst
  ```

  All changes to the configuration take effect automatically on the next boot, there is no need to re-run an activation program.

Example configuration:

```
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$O471l/$H/JW2MYeugX6Y1h3v.1Iz0

title linux
   kernel (hd0,1)/boot/vmlinuz root=/dev/sda2
   initrd (hd0,1)/boot/initrd
title failsafe
   lock
   kernel (hd0,1)/boot/vmlinuz.shipped root=/dev/sda2 ide=nodma apm=off \
      acpi=off vga=normal nosmp disableapic maxcpus=0 3
   initrd (hd0,1)/boot/initrd.shipped
```

The configuration shown here might not be exactly the configuration used on the installed system, depending on the kernel options needed for the hardware.

3.15.2 Yaboot boot loader configuration

Yaboot is used on the pSeries machines, it is an OpenFirmware-based boot loader, and can be reconfigured at boot time from a specialized command line.

Yaboot and GRUB are very similar, both support MD5-encrypted passwords specified in the configuration file.

You need to re-run the ybin(8) tool when you have modified the configuration file, this is however not necessary if you replace a kernel and keep all path names unchanged.

Please refer to the yaboot.conf(5) and ybin(8) manual pages and the yaboot HOWTO for more information:

```
http://penguinppc.org/projects/yaboot/doc/yaboot-howto.shtml
```

3.15.3 ZIPL boot loader configuration

The ZIPL boot loader is used on the zSeries mainframe when the system is set up using the VM virtualization layer. In this context, ”booting” refers to the initial program load (IPL) done from the CP command prompt, which affects only a single specific Linux instance (a.k.a. ”partition”, which refers to the running system and not the disk partition in this context).

Configuration of the VM system is beyond the scope of this document. You MUST ensure that the configuration settings and virtual devices used are only accessible to the authorized administrators. Do NOT use unencrypted 3270 sessions for console access on insecure networks.

ZIPL writes a boot record on the virtual disk (DASD) used by this Linux instance, this boot record then proceeds to load and run the Linux kernel itself. The `zipl` command must be re-run after any kernel or boot argument modifications. Please refer to the *zipl*(8) man page for more information.

```
# Generated by YaST2
[defaultboot]
default=ipl

[ipl]
target=/boot/zipl
image=/boot/kernel/image
ramdisk=/boot/initrd
parameters="dasd=0200 root=/dev/dasda1"
```

3.15.4 iSeries kernel slots

Similar to zSeries, the iSeries hosts use an initial program load (IPL) system to load and initialize a virtual Linux instance. There is no boot loader program on the Linux side, the host platform’s boot loader is configured through device drivers accessed via virtual files in the /proc file system.

Here is a sample session to copy a kernel to kernel slot B (usually reserved for experimental kernels, A is the production kernel), and activate it:

```
dd if=/boot/vmlinux.sm of=/proc/iSeries/mf/B/vmlinux bs=4k
cat /proc/cmdline > /proc/iSeries/mf/B/cmdline
echo "B" > /proc/iSeries/mf/side
```

For more information, please refer to:

```
http://www-1.ibm.com/servers/eserver/iseries/linux/tech_faq.html
```

3.16 Reboot and initial network connection

After all the changes described in this chapter have been done, you MUST reboot the system to ensure that all unwanted tasks are stopped, and that the running kernel, modules and applications all correspond to the evaluated configuration.

Please make sure that the boot loader is configured correctly for your platform. On zSeries, remember to run the *zipl*(8) tool to write the boot record.

The system will then match the evaluated configuration. The server MAY then be connected to a secure network as described above.

4 System operation

To ensure that the systems remains in a secure state, special care MUST be taken during system operation.

4.1 System startup, shutdown and crash recovery

Use the *shutdown*(8), *halt*(8) or *reboot*(8) programs as needed to shut down or reboot the system.

When powered on (or on initial program load of the logical partition on a host system), the system will boot into the SLES operating system. If necessary (i.e. after a crash), a filesystem check will be performed automatically. In rare cases manual intervention is necessary, please refer to the *e2fsck*(8) and *debugfs*(8) documentation for details in this case.

In case a nonstandard boot process is needed (for example booting from floppy disk or CD-ROM to replace a defective hard drive), interaction with the boot loader and/or the host's management system can be used to modify the boot procedure for recovery.

For example, on xSeries you can use the following grub commands launch a shell directly from the kernel, bypassing the normal init/login mechanism:

```
# view the current grub configuration
grub> cat (hd0,1)/boot/grub/menu.lst

# manually enter the modified settings
grub> kernel (hd0,1)/boot/vmlinuz root=/dev/sda1 init=/bin/sh
grub> initrd (hd0,1)/boot/initrd
grub> boot
```

Please refer to the relevant documentation of the boot loader, as well as the SuSE administrator guide, for more information.

4.2 Backup and restore

Whenever you make changes to security-critical files, you MAY need to be able to track the changes made and revert to previous versions, but this is not required for compliance with the evaluated configuration.

The *star*(1) archiver is RECOMMENDED for backups of complete directory contents, please refer to the section §6.5 "Data import / export". Regular backups of the following files and directories (on removable media such as CD-R, or on a separate host) are RECOMMENDED:

```
/etc/
/usr/lib/cracklib_dict.*
/var/spool/cron/
/var/spool/atjobs/
```

You MUST protect the backup media from unauthorized access, because the copied data does not have the access control mechanisms of the original file system. Among other critical data, it contains the secret keys used by the *SSH* and *stunnel* servers, as well as the */etc/shadow* password database. Store the backup media at least as securely as the server itself.

A RECOMMENDED method to track changes is to use a version control system. RCS is easy to set up because it does not require setting up a central repository for the changes, and you can use shell scripting to automate the change tracking. RCS is not included in the evaluated configuration, see *rcsintro*(1) in the rcs RPM package for more information. Alternatively, you can create manually create backup copies of the files and/or copy them to other servers using *scp*(1).

4.3 Gaining superuser access

System administration tasks require superuser privileges. Since directly logging on over the network as user 'root' is disabled, you MUST first authenticate using an unprivileged user ID, and then use the `su` command to switch identities. Note that you MUST NOT use the 'root' rights for anything other than those administrative tasks which require these privileges, all other tasks MUST be done using your normal (non-root) user ID.

You MUST use the *su*(1) command in exactly the following way to gain superuser access:

```
/bin/su -
```

This ensures that the correct binary is executed irrespective of PATH settings or shell aliases, and that the root shell starts with a clean environment not contaminated with the starting user's settings. This is necessary because the *.profile* shell configuration and other similar files are writable for the unprivileged ID, which would allow an attacker to easily elevate privileges to root if able to subvert these settings.

The administrator MUST NOT add any directory to the root user's PATH that are writable for anyone other than 'root', and similarly MUST NOT use or execute any scripts, binaries or configuration files that are writable for anyone other than 'root', or where any containing directory is writable for a user other than 'root'.

4.4 Installation of additional software

Additional software packages MAY be installed as needed from the SLES CDs, provided that they do not conflict with the security requirements.

Any additional software added is not intended to be used with superuser privileges. The administrator MUST use only those programs that are part of the original evaluated configuration for administration tasks, except if the administrator has independently ensured that use of the additional software is not a security risk.

Administrators MAY add scripts to automate tasks as long as those only depend on and run programs that are part of the evaluated configuration.

The security requirements for additional software are:

- Kernel modules MUST NOT be installed or loaded.
- Device special nodes MUST NOT be added to the system.
- setuid root or setgid root programs MUST NOT be added to the system. Programs which use setuid or setgid bits to run with identities other than 'root' MAY be added.
- The content, permissions and ownership of all existing filesystem objects (including directories and device nodes) that are part of the evaluated configuration MUST NOT be modified. Files and directories MAY be added to existing directories provided that this does not violate any other requirement.
- Programs automatically launched with 'root' privileges MUST NOT be added to the system. Exception: processes that *immediately* and *permanently* switch to a non privileged identity on launch are permitted, i.e. by using `su USERID -c LAUNCH_COMMAND` in the startup file, or alternatively by using the *setgroups*(2), *setgid*(2) and *setuid*(2) system calls in a binary. (*seteuid*(2) etc. are insufficient.)

  Automatic launch mechanisms are:

  - Entries in */etc/inittab*
  - Executable files or links in */etc/init.d/* and its subdirectories
  - Entries in */etc/xinetd.conf*
  - Scheduled jobs using `cron` (including entries in */etc/cron** files) or `at`.

Examples of programs that usually do not conflict with these requirements and therefore MAY be installed are compilers, interpreters, network services running with non-root rights, and similar programs. The requirements listed above MUST be verified in each specific case.

4.5 Scheduling processes using `cron` and `at`

The *cron*(8) program schedules programs for execution at regular intervals. Entries can be modified using the *crontab*(1) program - the file format is documented in the *crontab*(5) manual page.

You MUST follow the rules specified for installation of additional programs for all entries that will be executed by the 'root' user. Use non-root crontab entries in all cases where 'root' privileges are not absolutely necessary.

The *at*(1) and *batch*(1) programs execute a command line at a specific single point of time. The same rules apply as for jobs scheduled via *cron*(8). Use *atq*(1) and *atrm*(1) to manage the scheduled jobs.

Errors in the non interactive jobs executed by `cron` and `at` are reported in the system log files in */var/log/*, and additionally via e-mail to the user who scheduled it.

Permission for users to schedule jobs with `cron` and `at` is controlled through *allow* and *deny* files:

```
/etc/at.allow
/etc/at.deny
/var/spool/cron/allow
/var/spool/cron/deny
```

The *allow* file has precedence if it exists, then only those users whose usernames are listed in it are permitted to use the service. If it does not exist, the *deny* file is used instead and all users who are *not* listed in that file can use the service.

In the SLES distribution, the *allow* files do not exist, and *deny* files are used to prevent system-internal IDs and/or guest users from using these services. You MAY add to the *deny* files, but you MUST NOT remove any of the entries that were in the file as originally distributed.

You MAY create *allow* files (owner and group 'root', permissions 0600), but if you do so, you MUST NOT add any username to the *allow* file that is listed in the originally distributed *deny* file.

The distributed file */etc/at.deny* contains:

```
alias
backup
bin
daemon
ftp
games
gnats
guest
irc
lp
mail
man
nobody
operator
proxy
qmaild
qmaill
qmailp
qmailq
```

```
qmailr
qmails
sync
sys
www-data
```

The distributed file */var/spool/cron/deny* contains:

```
guest
gast
```

4.6 Mounting filesystems

If any filesystems need to be mounted in addition to those set up at installation time, the following mount options MUST be used if the filesystems contain data that is not part of the evaluated configuration:

```
nodev,nosuid,acl
```

This is necessary to ensure that mounting the filesystem does not introduce capabilities that could violate the security policy. Note that these settings do not completely protect against malicious code and data, therefore you MUST also verify that the data originates from a trustworthy source and does not compromise the server's security. Specifically, be aware of the following issues:

- Even unprivileged programs and scripts can contain malicious code that uses the calling user's rights in unintended ways, i.e. introducing trojan horses in the system, revealing confidential documents or corrupting the user's data.
- Data on the additional filesystem MUST have appropriate access rights to prevent disclosure to or modification by unauthorized users. Be aware that imported data may have been created using user names and permissions that do not match your system's security policies.

We RECOMMEND adding the *noexec* mount option to avoid accidental execution of files or scripts on additional mounted filesystems.

Disk space MAY be added by mounting empty filesystems created using `mkfs.ext3` and optionally moving existing files and directories onto them. The mount option `acl` MUST be specified for each additional ext3 filesystem.

The filesystem MUST be mounted on an empty directory that is not used for any other purpose. We RECOMMEND using a subdirectory of */mnt* for temporary disk mounts and subdirectories of */media* for removable storage media.

Example:

```
# mount /dev/cdrom /media/cdrom -t iso9660 -o nodev,nosuid,noexec
```

You MAY also add an equivalent configuration to */etc/fstab*, i.e.:

```
/dev/cdrom /media/cdrom iso9660 ro,noauto,nodev,nosuid,noexec 0 0
```

You MUST NOT use the *user* flag, ordinary users are not permitted to mount filesystems (this is also enforced by the deletion of the SUID bit on the *mount* command).

4.7 Managing user accounts

Use the *useradd*(8) command to create new user accounts, then assign a default password for the user (or alternatively permit the user to choose their own initial password if they are present). Refer to the manual pages for *useradd*(8) and *passwd*(1) for more information. User account names are at maximum 8 characters long. To force the user to choose a new password immediately after the first login, the time of the last change of the password MUST be set with the *chage* command.

Example:

```
useradd -m -c "John Doe" jdoe
passwd jdoe
chage -d 1970-01-01 jdoe
```

If necessary, you MAY reset the user's password to a known value using `passwd` *`USER`*, and entering the new password. You cannot recover the previously used password, since the hash function used is not reversible.

You MAY use the *usermod*(8) command to change a user's properties. For example, if you want to add the user 'jdoe' to the *trusted* group, you could use the following:

```
# List the groups the user is currently a member of:
groups jdoe

# Add the additional group
usermod -G $(su jdoe -c groups | sed 's/ /,/g'),trusted jdoe
```

Users MAY be locked out (disabled) using `passwd -l` *`USER`*, and re-enabled using `passwd -u` *`USER`*.

The *chage*(1) utility MAY be used to view and modify the expiry settings for user accounts. Unprivileged users are able to view but not modify their own expiry settings.

The *userdel*(8) utility removes the user account from the system, but does not remove files outside the home directory (and the mail spool file), or kill processes belonging to this user. Use `kill` (or reboot the system) and `find` to do so manually if necessary, i.e.:

```
# Which user to delete?
U=jdoe

# Lock user account, but don't remove it yet
passwd -l $U

# Kill all user processes, repeat if needed (or reboot)
kill -9 `ps -la --User $u|awk '{print $4}'`

# Recursively remove all files and directories belonging to user
# (Careful - this may delete files belonging to others if they
# are stored in a directory owned by this user.)
find / -depth \( ! -fstype ext3 -prune -false \) \
        -o -user $U -exec rm -rf {} \;

# Remove cron and at jobs
crontab -u $U -r
find /var/spool/atjobs -user $U -exec rm {} \;
```

```
# Now delete the account
userdel $U
```

You MAY specify a script that *userdel* executes when deleting users in */etc/login.defs*.

If you need to create additional groups or modify existing groups, use the *groupadd*(8), *groupmod*(8) and *groupdel*(8) commands.

Group passwords are NOT supported in the evaluated configuration, and have been disabled by removing the setuid bit from the *newgrp*(8) program. You MUST NOT re-enable this feature and MUST NOT use *passwd*(1) with the `-g` switch or the *gpasswd*(1) command to set group passwords.

When creating a new user, you will define an initial password for this user. You MUST transfer this initial password in a secure way to the user, ensuring that no third party gets the information. For example, you can tell the password to a user personally known to you. If this is not possible, you MAY send the password in written form in a sealed letter. This applies also when you set a new password for a user (i.e. in case the user has forgotten his password). You need to advise the user that he MUST change this initial password when he first logs into the system and select his own password in accordance with the rules defined in section §6.3 ”Password policy”.

4.8 SYSV shared memory and IPC objects

The system supports SYSV-compatible shared memory, IPC objects and message queues. If programs fail to release resources they have used (i.e. due to a crash), the administrator MAY use the *ipcs*(8) utility to list information about them, and *ipcrm*(8) to force deletion of unneeded objects. Note that these resources are also released when the system is rebooted.

For additional information, please refer to the *msgctl*(2), *msgget*(2), *msgrcv*(2), *msgsnd*(2), *semctl*(2), *semget*(2), *semop*(2), *shmat*(2), *shmctl*(2), *shmdt*(2), *shmget*(2) and *ftok*(3) manual pages.

4.9 Configuring secure network connections with *stunnel*

4.9.1 Introduction

The *stunnel* program is a flexible and secure solution for setting up encrypted network connections, enabling the use of strong encryption even for applications that are not able to use encryption natively. *stunnel* uses the OpenSSL library for its encryption functions, and the corresponding *openssl*(1) command line tool for key management.

Stunnel has three main operating modes:

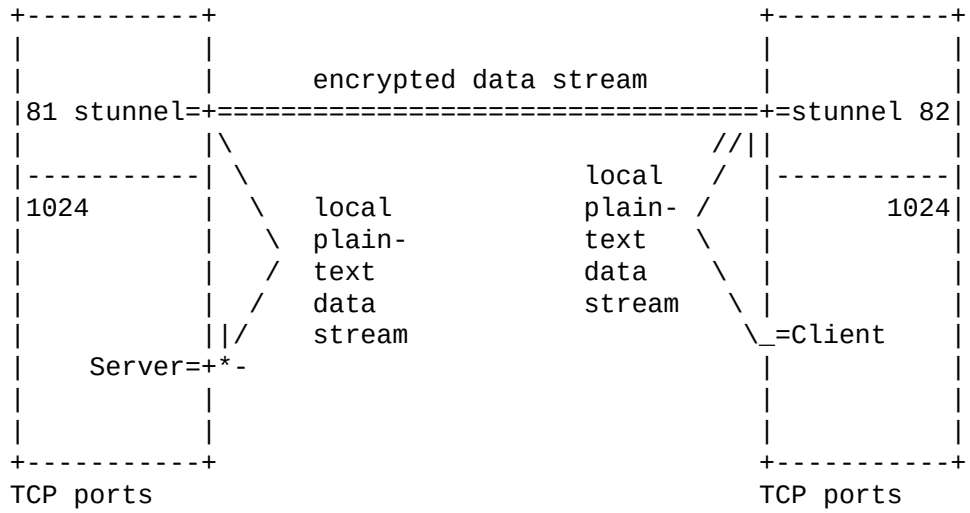
- Accept incoming SSL-encrypted TCP connections, and run a specific program to handle the request.

  This is similar to how *xinetd* launches programs, and any program compatible with *xinetd* can also be used for this purpose. It must read and write the communication data on the *stdin* and *stdout* file descriptors and stay in the foreground. *stunnel* also supports switching user and group IDs before launching the program.

- Open a SSL connection to a remote SSL-capable TCP server, and copy data to and from *stdin* and *stdout*.

- Bind a TCP port to accept incoming unencrypted connections, and forward data using SSL to a prespecified remote server.

The following diagram shows a sample usage scenario:



In this scenario, neither the client nor the server have administrator privileges, they are running as normal user processes. Also, the client and server do not support encryption directly.

stunnel makes a secure communication channel available for the client and server. On the client, *stunnel* is accepting connections on TCP port 82. The client connects to this port on the local machine using normal unencrypted TCP, *stunnel* accepts the connection, and opens a new TCP connection to the *stunnel* server running on the remote machine. The *stunnel* instances use cryptographic certificates to ensure that the data stream has not been intercepted or tampered with, and then the remote *stunnel* opens a third TCP connection to the server, which is again a local unencrypted connection.

Any data sent by either the client or server is accepted by the corresponding *stunnel* instance, encrypted, sent to the other *stunnel*, decrypted and finally forwarded to the receiving program. This way, no modifications are required to the client and server.

To set up a secure connection compliant with the evaluated configuration, you MUST start the *stunnel* server(s) with administrator rights, and you MUST use a TCP port in the administrator-reserved range 1-1023 to accept incoming connections.

stunnel MAY also be used to set up encrypted connections by non-administrative users using ports in the range 1024-65536. This is permitted, but it is outside of the scope of the evaluated configuration and not considered to be a trusted connection.

Any network servers and clients other than the trusted programs described in this guide (*stunnel*, *sshd*, *vsftpd* (run via *xinetd*), *postfix* and *lpd*) MUST be run using non-administrator normal user identities. Programs run from *stunnel* MUST be switched to a non-root user ID by using the `-s` and `-g` flags.

We RECOMMEND configuring any such servers to accept connections only from machine-local clients, either by binding only the *localhost* IP address 127.0.0.1, or by software filtering inside the application. This ensures that the only encrypted connections are possible over the network. Details on how to do this depend on the software being used and are beyond the scope of this document.

Please refer to the *stunnel*(1) and *openssl*(1) man pages for more information.

4.9.2 Creating an externally signed certificate

We strongly RECOMMEND that you have your server's certificate signed by an established Certificate Authority (CA), which acts as a trusted third party to vouch for the certificate's authenticity for clients. Please refer to the *openssl*(1) and req(1) man pages for instructions on how to generate and use a certificate signing request.

Create the server's private key and a certificate signing request (CSR) with the following commands:

```
touch /etc/stunnel/stunnel.pem

chmod 400 /etc/stunnel/stunnel.pem

openssl req -newkey rsa:1024 -nodes \
  -config /usr/share/doc/packages/stunnel/stunnel.cnf \
  -keyout /etc/stunnel/stunnel.pem -out /etc/stunnel/stunnel.csr
```

You will be prompted for the information that will be contained in the certificate. Most important is the ”Common Name”, because the connecting clients will check if the hostname in the certificate matches the server they were trying to connect to. If they do not match, the connection will be refused, to prevent a ’man-in-the-middle’ attack.

Here is a sample interaction:

```
Using configuration from /usr/share/doc/packages/stunnel/stunnel.cnf
Generating a 1024 bit RSA private key
..........++++++
.......++++++
writing new private key to '/etc/stunnel/stunnel.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [PL]:US
State or Province Name (full name) [Some-State]:TX
Locality Name (eg, city) []:Austin
Organization Name (eg, company) [Stunnel Developers Ltd]:Example Inc.
Organizational Unit Name (eg, section) []:
Common Name (FQDN of your server) []:www.example.com
Common Name (default) []:localhost
```

The file */etc/stunnel/stunnel.pem* will contain both the certificate (public key) and also the secret key needed by the server. The secret key will be used by non-interactive server processes, and therefore cannot be protected with a passphrase. You MUST protect the secret key from being read by unauthorized users, to ensure that you are protected against someone impersonating your server.

Next, send the generated CSR file */etc/stunnel/stunnel.csr* (*not* the private key) to the CA along with whatever authenticating information they require to verify your and your server's identity. The CA will then generate a signed certificate from the CSR, using a process analogous to `openssl req -x509 -in stunnel.csr -key CA-key.pem -out signed-cert.pem`.

When you receive the signed certificate back from the CA, append it to the file */etc/stunnel/stunnel.pem* containing the private key:

```
cat signed-cert.pem >> /etc/stunnel/stunnel.pem
```

Make sure that the resulting file contains no extra whitespace or other text in addition to the key and certificate:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCzF3ezbZFLjgv1YHNXnBnI8jmeQ5MmkvdNw9XkLnA2ONKQmvPQ
[...]
4tjzwTFxPKYvAW3DnXxRAkAvaf1mbc+GTMoAiepXPVfqSpW2Qy5r/wa04d9phD5T
oUNbDU+ezu0Pana7mmmvg3Mi+BuqwlQ/iU+G/qrG6VGj
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIC1jCCAj+gAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGEwJQTDET
[...]
bIbYKL6Q1kE/vhGmRXcXQrZzkfu8sgJv7JsDpoTpAdUnmvssUY0bchqFo4Hhzkvs
U/whL2/8RFv5jw==
-----END CERTIFICATE-----
```

You MAY distribute the original signed certificate (*signed-cert.pem* in this example) to clients, it does not contain any confidential information. *Never* distribute the file containing the private key, that is for use by the `stunnel` server only.

4.9.3 Creating a self-signed certificate

Alternatively, you MAY use a self-signed certificate instead of one signed by an external CA. This saves some time and effort when first setting up the server, but each connecting client will need to manually verify the certificate's validity. Experience shows that most users will not do the required checking and simply click "OK" for whatever warning dialogs that are shown, resulting in significantly reduced security. Self-signed certificates can be appropriate for controlled environments with a small number of users, but are not recommended for general production use.

Create a self-signed host certificate with the following commands:

```
touch /etc/stunnel/stunnel.pem

chmod 400 /etc/stunnel/stunnel.pem

openssl req -new -x509 -days 365 -nodes \
  -config /usr/share/doc/packages/stunnel/stunnel.cnf \
  -out /etc/stunnel/stunnel.pem -keyout /etc/stunnel/stunnel.pem
```

The secret key contained in this file MUST be kept secret.

You MAY extract the public certificate from this file for distribution to clients. Make sure you do not accidentally distribute the secret key:

```
sed '1,/END/d' < /etc/stunnel/stunnel.pem > signed-cert.pem
```

The client has no independent way to verify the validity of a self-signed certificate, therefore each client MUST manually verify and confirm the validity of the certificate.

One method is to give a copy of the self-signed certificate to the client (using a secure transport mechanism, not e-mail), and import it into the client directly. The `stunnel` client uses the *-A* and *-a* options for this purpose.

Alternatively, many client programs (not `stunnel`) can interactively import the certificate when connecting to the server. The client will display information about the server's certificate including an MD5 key fingerprint. You need to compare this fingerprint with the original fingerprint of the server's certificate.

Run the following command on the server to display the original certificate's fingerprint:

```
openssl x509 -fingerprint -in /etc/stunnel/stunnel.pem
```

Most clients will store the certificate for future reference, and will not need to do this verification step on further invocations.

4.9.4 Activating the tunnel

In the evaluated configuration, you MUST use the following cipher suite as defined in the SSL v3 protocol:

```
RC4-SHA       = SSL_RSA_WITH_RC4_128_SHA (SC1.8)
```

stunnel does not support a central configuration file, therefore you MUST specify the supported cipher by using the `-C` command line flag on each invocation of the *stunnel* client or server:

```
stunnel -C RC4-SHA ...
```

For a service or tunnel that will only be used temporarily, simply launch the `stunnel` program from the command line. The tunnel will be available for multiple clients, but will not be started automatically after a reboot. To shut down the tunnel again, search for the command line in the `ps ax` process listing and kill the PID shown:

```
kill ‘ps ax | grep -v grep | grep ’stunnel.*-d 495’ | awk ’{print $1}’‘
```

Permanent tunnels MAY be added to */etc/inittab*, these will be re-launched automatically whenever they are terminated, as well as after a reboot. Use this method for both client and server *stunnel* trusted instances, using the `-c` and `-d` flags appropriately:

```
s1:respawn:/usr/sbin/stunnel -f [FLAGS] >>/var/log/stunnel.s1.log 2>&1
s2:respawn:/usr/sbin/stunnel -f [FLAGS] >>/var/log/stunnel.s2.log 2>&1
```

Use the same *FLAGS* as when running from the command line, but add the `-f` (foreground) flag (otherwise `init` will misinterpret the backgrounded server as having died and will try to restart it immediately, causing a loop), and redirect the output to a log file.

4.9.5 Using the tunnel

If the client program supports SSL encryption, it will be able to communicate with the *stunnel* service directly. You will need to verify and accept the server’s certificate if the client cannot recognize it as valid according to its known certification authorities.

If the client program does not support SSL directly, you can use `stunnel` as a client, or indirectly by setting up a proxy that allows the client to connect to an unencrypted local TCP port.

WARNING: The `stunnel` client does *not* verify the server’s certificate by default. You MUST specify either `-v 2` or `-v 3` on the client command line to switch on certificate verification.

As described in the previous section, you MUST use the `-C RC4-SHA` command line parameter to ensure that the cipher selection supported in the evaluated configuration will be used.

You MAY also activate client certificate verification for the server to verify the client’s identity.

4.9.6 Example 1: system status view

As administrator, install a server on TCP port 81 that accepts SSL connections and reports the server’s memory usage statistics to connecting clients:

```
stunnel -C RC4-SHA -d 81 -g nogroup -s nobody \
    -l /usr/bin/free -- free
```

As a normal user, run `stunnel` in client mode to connect to the server and retrieve the information:

```
stunnel -C RC4-SHA -A signed-cert.pem -v 3 -c \
    -r 127.0.0.1:81
```

Other information services can be added in a similar fashion by adding more stunnel servers with appropriate command lines.

4.9.7 Example 2: Using outbound encryption with a non-encrypting client

This example shows how the standard `telnet` client can be used to retrieve information from an SSL-enabled server. It assumes that the ”free” server is running as described in the previous example.

As administrator, set up a proxy that accepts unencrypted connections on TCP port 82 and forwards the data using SSL to the (remote) server on port 81:

```
stunnel -C RC4-SHA -A signed-cert.pem -v 3 -c -d 82 \
     -r 127.0.0.1:81
```

Then, as a normal user, use unencrypted ”telnet” to connect to the proxy:

```
telnet localhost 82
```

4.9.8 Example 3: Secure SMTP delivery

Normal SMTP e-mail delivery is not encrypted, but most mail clients support the enhanced SMTPS protocol that uses SSL encryption. The protocol itself is unchanged other than being encrypted.

`stunnel` can easily be used as a proxy to receive SMTPS connections on the standard port expected by clients (465/tcp), and then forward the data to the mail server listening on the SMTP port (25/tcp). The mail server configuration does not need to be modified to support encryption of incoming mail. Run the following command as administrator:

```
stunnel -C RC4-SHA -d 465 -r 25
```

4.10 The Abstract Machine Testing Utility (AMTU)

The security of the operating system depends on correctly functioning hardware. For example, the memory subsystem uses hardware support to ensure that the memory spaces used by different processes are protected from each other.

The Abstract machine Testing Utility (AMTU) is distributed as an RPM inside the certification-sles-eal3 RPM, and was installed previously as described in the section §3.2 ”Add and remove packages”.

To run all supported tests, simply execute the `amtu` program:

```
# amtu
Executing Memory Test...
Memory Test SUCCESS!
Executing Memory Separation Test...
Memory Separation Test SUCCESS!
Executing Network I/O Tests...
Network I/O Controller Test SUCCESS!
```

```
Executing I/O Controller - Disk Test...
I/O Controller - Disk Test SUCCESS!
Executing Supervisor Mode Instructions Test...
Privileged Instruction Test SUCCESS!
```

The program will return a nonzero exit code on failure, which MAY be used to automatically detect failures of the tested systems and take appropriate action.

Please refer to the *amtu*(8) man page for more details.

5 Monitoring, Logging & Audit

5.1 Reviewing the system configuration

We RECOMMEND that you review the system's configuration at regular intervals to verify if it still agrees with the evaluated configuration. This primarily concerns those processes that may run with 'root' privileges.

The permissions of the device files */dev/** MUST NOT be modified.

In particular, review settings in the following files and directories to ensure that the contents and permissions have not been modified:

```
/etc/at.allow
/etc/at.deny
/etc/audit/*
/etc/cron.d/*
/etc/cron.daily/*
/etc/cron.hourly/*
/etc/cron.monthly/*
/etc/cron.weekly/*
/etc/crontab
/etc/ftpusers
/etc/group
/etc/gshadow
/etc/hosts
/etc/init.d/*
/etc/inittab
/etc/ld.so.conf
/etc/login.defs
/etc/modules.conf
/etc/pam.d/*
/etc/passwd
/etc/securetty
/etc/security/pam_pwcheck.conf
/etc/security/pam_unix2.conf
/etc/shadow
/etc/ssh/ssh_config
/etc/ssh/sshd_config
/etc/sysconfig/*
/etc/vsftpd.conf
/etc/xinetd.conf

/usr/lib/cracklib_dict.*
```

```
/var/log/audit.d/*
/var/spool/atjobs/*
/var/spool/cron/*
/var/spool/cron/allow
/var/spool/cron/deny
```

Use the command `lastlog` to detect unusual patterns of logins.

Also verify the output of the following commands (run as 'root'):

```
atq
crontab -l
find / \( -perm -4000 -o -perm -2000 \) -ls
find / \( -type f -o -type d -o -type b \) -perm -0002 -ls

find /bin /boot /etc /lib /sbin /usr \
        ! -type l \( ! -uid 0 -o -perm +022 \)
```

5.2 System logging and accounting

System log messages are stored in the */var/log/* directory tree in plain text format, most are logged through the *syslogd*(8) and *klogd*(8) programs, which MAY be configured via the file */etc/syslog.conf*.

The *logrotate*(8) utility, launched from */etc/cron.daily/logrotate*, starts a fresh log file every week or when they reach a maximum size and automatically removes or archives old log files. You MAY change the configuration files */etc/logrotate.conf* and */etc/logrotate.d/** as required.

In addition to the *syslog* messages, various other log files and status files are generated in */var/log* by other programs:

```
File           Source
YaST2          Directory for YaST2 log files
audit.d        Directory for LAuS logs
boot.msg       Messages from system startup
lastlog        Last successful log in  (see lastlog(8))
vsftpd.log     Transaction log of the VSFTP daemon
localmessages  Written by syslog
mail           Written by syslog, contains messages from the MTA (postfix)
messages       Written by syslog, contains messages from su and ssh
news/          syslog news entries (not used in the evaluated configuration)
warn           Written by syslog
wtmp           Written by the PAM susbystem, see who(1)
xinetd.log     Written by xinetd, logging all connections
```

Please see *syslog*(3), *syslog.conf*(5) and *syslogd*(8) man pages for details on syslog configuration.

The *ps*(1) command can be used to monitor the currently running processes. Using `ps faux` will show all currently running processes and threads.

5.3 Configuring the audit subsystem

The audit subsystem implements a central monitoring solution to keep track of security relevant events, such as changes and change attempts to security critical files.

This is accomplished through two separate mechanisms. All system calls are intercepted, and the kernel writes the parameters and return value to the audit log for those calls that are marked as security relevant in the filter configuration. In addition, some trusted programs contain audit-specific code to write audit trails of the actions they are requested to perform.

Please see *auditd*(8), *laus*(7), *auditd.conf*(5), *aucat*(8) and *augrep*(8) for details.

5.3.1 Intended usage of the audit subsystem

CAPP (the Controlled Access Protection Profile) specifies the auditing capabilities that a compliant system must support. The evaluated configuration described here is based on these requirements.

WARNING: Some of the CAPP requirements may conflict with your specific requirements for the system. For example, a CAPP-compliant system MUST disable logins if the audit subsystem is not working. Please ensure that you are aware of the consequences if you enable auditing.

CAPP is designed for a multiuser system, with multiple unique users who maintain both shared and private resources. The auditing features are intended to support this mode of operation with a reliable trail of security-relevant operations. It is less useful for a pure application server with no interactive users.

Please be aware that the auditing subsystem will, when activated, cause some slowdown for applications on the server. The impact depends on what the application is doing and how the audit subsystem is configured. As a rule of thumb, applications that open a large number of separate files are most affected, and CPU-bound programs should not be measurably affected. You will need to balance the performance requirements against your security needs when deciding if and how you want to use auditing.

5.3.2 Selecting the events to be audited

You MAY make changes to the set of system calls and events that are to be audited. CAPP requires that the system has the *capability* to audit security relevant events, but it is up to you to choose how you want to use these capabilities. It is acceptable to turn off system call auditing completely even in an evaluated configuration, for example on a pure application server with no interactive users on the system.

The configuration file */etc/audit/filter.conf* by default contains a suggested setup for a typical multiuser system, all access to the security relevant files (as configured in */etc/audit/eal3files.conf*) is audited, along with other security relevant events such as system reconfiguration.

You MAY selectively disable and enable auditing for specific events or users as required by setting up predicates and filters in the *filter.conf* file. The following excerpt from the default configuration is an example:

```
predicate is-non-root-uid = !eq(0);
filter not-root-user = is-non-root-uid(login-uid);

tag "Open_Denied"
syscall open = denied(result)
              && (( not-root-user || effectivenonroot )
              && is-sysdir(arg0));
```

Please refer to the *audit-filter*(5) man page for more details.

5.3.3 Reading and searching the audit records

Use the *aucat*(8) and *augrep*(8) tools to retrieve information from the audit logs. The information available for retrieval depends on the active filter configuration. If you modify the filter configuration, we RECOMMEND keeping a datestamped copy of the applicable configuration with the log files for future reference.

For example:

```
# view the last 100 audit records
aucat | tail -100

# view all successful PAM authentications
augrep -e TEXT -U AUTH_success

# all actions recorded for a specified login UID (this includes
# actions done by this user with a different effective UID,
# i.e. via setuid programs or as part of a "su" session)
augrep -l kw

# file removals
augrep -e SYSCALL -S unlink
```

Of course, you can use other tools such as plain *grep*(1) or scripting languages such as *awk*(1), *python*(1) or *perl*(1) to further analyze the text output generated by the low-level audit tools.

5.3.4 Starting and stopping the audit subsystem

The audit subsystem is only active when all of the following conditions are met:

- The *audit.o* kernel module must be loaded.
- The audit daemon `auditd` must be running.
- Processes are attached to the audit subsystem by explicitly launching them with the *aurun*(8) wrapper program; starting them from an interactive shell session that used the *pam_laus.so* PAM module when logging in; or when syscall auditing is enabled globally for all processes (setting *AUDIT_ATTACH_ALL=1* in */etc/sysconfig/audit*).

If the audit daemon is terminated, no audit events are generated until it is restarted. To avoid lost audit records when you have modified the filter configuration, you MUST use the command `auditd -r` to re-load the filters.

WARNING: `auditd -r` will *not* reload */etc/audit/audit.conf*, it only reloads the filter configuration file. To activate changes to this configuration file, you MUST restart the audit daemon:

```
/etc/init.d/audit restart
```

You MUST NOT attempt to reload the configuration by sending *auditd* a *HUP* signal or by running `/etc/init.d/audit reload`, because that will not write the required audit record showing the reconfiguration. You MUST use one of the two restart methods described above.

If the audit module is unloaded with `rmmod`, all processes are detached permanently from the audit subsystem. They can only be re-attached when using the *AUDIT_ATTACH_ALL=1* option in */etc/sysconfig/audit*.

5.3.5 Storage of audit records

The RECOMMENDED operating mode for the audit records is ”bin mode” (”bin” as in bucket), using several preallocated files of constant size for the audit records. `auditd` will write data to the first file, and once it is filled switch to the next one, re-using each one in turn in a round-robin fashion.

Each time a bin is filled, `auditd` will launch the configured notification program to process the file. The default configuration saves a copy of each filled file before re-using the storage. If the notification program exits with a failure status, i.e. due to lack of disk space, `auditd` will then take the configured action, by default setting the message queue size to zero and thereby blocking all processes that try to write new records. These audited processes will sleep until `auditd` resumes processing (i.e. once disk space has been freed by the administrator), then they will be woken up by the kernel and proceed running normally.

You MAY instead configure round-robin reuse of the files without saving, to keep the disk space used by the audit logs constant. To do that, remove the ”-S /var/log/audit.d/save.%u” option in */etc/audit/audit.conf*. In this configuration, you have access to a fixed amount of historical audit data, but any new events will cyclically overwrite old data. A user could exploit this mechanism by intentionally generating a large number of irrelevant entries to wipe out the previously generated records.

5.3.6 Reliability of audit data

By default, the audit records are written using the normal Linux filesystem buffering, which means that information may be lost in a crash because it has not been written to the physical disk yet. Any applications that read the records while the system is running will always get the most current data out of the buffer cache, even if it has not yet been committed to disk, so this does not affect normal operation. If you want to ensure that auditd always forces a disk write for each record, you MAY set the ”sync = yes;” option in */etc/audit/audit.conf*, but be aware that this will result in significantly reduced performance and high strain on the disk.

The audit record files are *not* protected against a malicious administrator, and are not intended for an environment where the administrators are not trustworthy.

5.4 System configuration variables in */etc/sysconfig*

The system uses various files in */etc/sysconfig* to configure the system. Most files in this directory tree contain variable definitions in the form of shell variables that are either read by the rc scripts at system boot time or are evaluated by the `SuSEconfig` command and used as input to re-write other configuration files on the system.

The following is a brief overview of the security relevant files, including the specification of permitted changes.

In the evaluated configuration, no changes are permitted that would require running the `SuSEconfig` command to re-write other configuration files. You MAY run `SuSEconfig`, but it will have no effect on the evaluated configuration.

5.4.1 *suseconfig*

This file specifies global configuration variables. Most notably ENABLE_SUSECONFIG, which specifies whether *SuSEconfig* is allowed to modify other configuration files based on the variables in */etc/sysconfig*.

Security relevant entries that MUST NOT be changed are:

```
ENABLE_SUSECONFIG="yes"  Is SuSEconfig allowed to modify configuration files?
MAIL_REPORTS_TO="root"   Where are system status mails sent to
CWD_IN_ROOT_PATH="no"    There MUST NOT be an entry for the current directory
CWD_IN_USER_PATH="no"    There MUST NOT be an entry for the current directory
```

5.4.2 *security*

Specifies the operation mode and the configuration file for the SuSE permission system. Read by the *chkstat*(8) program which is run automatically by `yast2` after installation of new software. The following settings MUST NOT be changed:

```
CHECK_PERMISSIONS=set
PERMISSION_SECURITY="eal3"
```

5.4.3 *cron*

Configures standard system cron jobs, like deletion of old files in */tmp* or update of the *man* databases. The settings are read by the shell scripts */etc/cron.daily/**. Security relevant variables are the following settings which MUST NOT be changed:

```
MAX_DAYS_IN_TMP=0                   How many days can files stay in /tmp
TMP_DIRS_TO_CLEAR="/tmp /var/tmp"   Which temporary directories are checked
OWNER_TO_KEEP_IN_TMP="root"         Ids for which files will not be erased
CLEAR_TMP_DIRS_AT_BOOTUP="no"       No cleaning of temp directories at boot
```

5.4.4 *language*

Sets up the default locale. This MUST NOT be changed, non-root users MAY override these default settings in their shell profiles.

5.4.5 *backup*

Configures the backup of the RPM database. MAY be changed.

5.4.6 *boot*

Configures the verbosity and interaction level of the boot process for debugging. Read by bootup scripts in */etc/init.d/*. MAY be changed.

5.4.7 *displaymanager*

This would configure the display manager for a workstation. It is not used in the evaluated configuration.

5.4.8 *kernel*

Configures modules to be installed in the initrd for system boot. MUST NOT be changed.

5.4.9 *clock*

Configures time zone and system clock, read during system boot. MAY be changed.

5.4.10 *proxy*

Configures global variables for the use of proxies. Not used in the evaluated configuration.

5.4.11 *windowmanager*

Would select the window manager on a workstation. Not used in the evaluated configuration.

5.4.12 *sysctl*

Configures some system variables for the boot process. The following are security relevant and MUST NOT be changed:

```
IP_DYNIP=no             The system only has a static address
IP_TCP_SYNCOOKIES=yes   Syn Flood protection
IP_FORWARD=no           Has to be set to yes if the system acts as a router.
ENABLE_SYSRQ=no         System request key MUST be disabled.
```

5.4.13 *java*

Would configure the Java run time environment if installed. Not used in the evaluated configuration.

5.4.14 *mail*

Configures the MTA.

Security relevant variables that MUST NOT be changed are:

```
SMTPD_LISTEN_REMOTE="no"    If set to yes, SuSEconfig will tell postfix to
                            accept remote connections.
```

5.4.15 *hardware*

Configures hardware parameters (DMA), read during system boot. MAY be changed.

5.4.16 *printer*

Sets the default printer. MUST NOT be changed, but non-root users may override the setting in their shell profiles.

5.4.17 *news*

Usenet news / NNTP settings. Not used in the evaluated configuration.

5.4.18 *console*

Sets up the console configuration (font, code page, frame buffer). MUST NOT be changed.

5.4.19 *keyboard*

Sets up the console keyboard (repeat rate, layout, number of virtual consoles). MAY be changed.

5.4.20 *mouse*

Sets up the mouse type. Not used in the evaluated configuration.

5.4.21 *lvm*

Sets up LVM. Not used in the evaluated configuration.

5.4.22 *network*

This directory contains the networking configuration and scripts for the interfaces and routes. MAY be modified as needed, but IP addresses MUST be static (no DHCP).

5.4.23 *syslog*

Configures the *syslog* daemon. MAY be changed.

5.4.24 *SuSEfirewall2*

Configures the SuSE firewall. Not used in the evaluated configuration.

5.4.25 *hotplug*

Configures dynamically attached devices (USB, Firewire). Not used in the evaluated configuration.

5.4.26 *ssh*

Configures command line options for the SSH daemon. MUST NOT be changed.

5.4.27 *postfix*

Configures the basic MTA setup. MUST NOT be changed.

5.4.28 *bootloader*

Configures the type of bootloader to use and where to store the boot record. MUST NOT be changed.

5.4.29 *audit*

Configures tunable paramaters for the kernel part of the audit subsystem. MUST NOT be changed.

6 Security guidelines for users

6.1 Online Documentation

The system provides a large amount of online documentation, usually in text format. Use the `man` program to read entries in the online manual, i.e.:

```
man ls
man man
```

to read information about the `ls` and `man` commands respectively. You can search for keywords in the online manual with the *apropos*(1) utility, i.e.:

```
apropos password
```

When this document refers to manual pages, it uses the syntax ENTRY(SECTION), i.e. *ls*(1). Usually you do not need to provide the section number, but if there are several entries in different sections, you can use the optional `-S` switch and pick a specific one.

Some programs provide additional information GNU 'texinfo' format, use the `info` program to read it, i.e.:

```
info diff
```

Additional information, sorted by software package, can be found in the directories */usr/share/doc/packages/*/*. Use the *less*(1) pager to read it, i.e.:

```
/usr/share/doc/packages/gpg/FAQ
```

Many programs also support a `--help`, `-?` or `-h` switch you can use to get a usage summary of supported command-line parameters.

A collection of How-To documents in HTML format can be found under */usr/share/doc/howto/en/html* if the optional *howtoenh* package is installed.

Please see */usr/share/doc/howto/en/html/Security-HOWTO* for security information. The HTML files can be read with the *w3m* browser.

The SuSE Linux Enterprise server documentation is also installed in electronic form. */usr/share/doc/packages/sles-inst-x86+x86-64_en/* contains the installation guide in PDF format, and */usr/share/doc/packages/sles-admin-x86+x86-64_en/* the administration manual. Note that the Security Guide (this document) has precedence over other documents in case of conflicting recommendations.

6.2 Authentication

You MUST authenticate (prove your identity) before being permitted to use the system. When the administrator created your user account, he or she will have assigned a user name and default password, and provided that information for you along with instructions how to access the system.

Logging in to the system will usually be done using the Secure Shell (SSH) protocol, alternatively a serial terminal may be available. Use the `ssh` command to connect to the system unless instructed otherwise by the administrator, for example:

```
ssh jdoe@172.16.0.1
```

The *ssh*(1) manual page provides more information on available options. If you need to transfer files between systems, use the *scp*(1) or *sftp*(1) tools.

If this is the first time you are connecting to the target system, you will be prompted if you want to accept the host key. If the administrator has provided a key fingerprint for comparison, verify that they match, otherwise type `yes` to continue. You MUST immediately change your initially assigned password with the *passwd*(1) utility.

You MUST NOT under any circumstances attempt to log in from an insecure device, such as a public terminal or a computer belonging to a friend. Even if the *person* owning the computer is trustworthy, the *computer* may not be due to having been infected with malicious code. Always remember that the device you are typing your password into has the ability to save and re-use your authentication information, so you are in effect giving the computer you are using the right to do any and all actions in your name. Insecure handling of authentication information is the leading cause for exploits of otherwise secure systems, and SSH can only protect the information during transit, and offers no protection at all against an insecure end point.

When you log out from the system and leave the device you have used for access (i.e. a terminal or a workstation with terminal emulation), you MUST ensure that you have not left information on the screen or within an internal buffer that should not be accessible to another user. You should be aware that some terminals also store information not displayed on the terminal (i.e. passwords, or the contents of a scrollback buffer). Nevertheless this information may be extractable by the next user unless the terminal buffer has been cleared.

If you ever forget your password, contact your administrator, who will be able to assign a new password.

You MAY use the *chsh*(1) and *chfn*(1) programs to update your login shell and personal information if necessary. Not all settings can be changed this way, contact your administrator if you need to change settings that require additional privileges.

6.3 Password policy

All users MUST ensure that their authentication passwords are strong (hard to guess) and handled with appropriate security precautions. The password policy described here is designed to satisfy the requirements of the evaluated configuration. If your organization already has a password policy defined, your administrator MAY refer you to that policy if it is equivalently strong.

You MUST change the initial password set by the administrator when you first log into the system. You MUST select your own password in accordance with the rules defined here. You MUST also change the password if the administrator has set a new password (i.e. if you have forgotten your password and requested the administrator to reset the password).

- Your password MUST be a minimum of 8 characters in length. More than 8 characters MAY be used (it is RECOMMENDED to use more than 8, best is to use passphrases), and all characters are significant.
- Use at least one character each from the following sets:

```
Lowercase letters: abcdefghijklmnopqrstuvwxyz
Uppercase letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Digits:            0123456789
Punctuation:       !"#$%&'()*+,-./:;<=>?[\]^_`{|}~
```

- You MUST NOT base the password on a dictionary word, your real name, login name, or other personal details (such as dates, names of relatives or pets), or names of real people or fictional characters.
- You MUST NOT use a simple alphabetic string, palindrome or combinations of adjacent keyboard keys.
- When you choose a new password, it MUST NOT be a simple variation or permutation of a previously used one.

- You MUST NOT write the password on paper or store it on electronic devices in unprotected form. Storage in a secure location (i.e. envelope in safety deposit box, or encrypted on an electronic device) MAY be acceptable, contact your administrator first to ensure that the protection is strong enough to make password recovery infeasible for the types of attackers the system is intended to protect against.
- The password is for you and you only. A password is like a toothbrush - you do not want to share it with anybody, even your best friend. You MUST NOT disclose your password to anybody else, or permit anybody else to use the system using your identity.

  Note that administrators will never ask you for your password, since they do not need it even if they are required to modify settings affecting your user account.
- You MUST NOT use the same password for access to any systems under external administration, including Internet sites. You MAY however use the same password for accounts on multiple machines within one administrative unit, as long as they are all of an equivalent security level and under the control of the same administrators.
- You MUST inform the administrator and select a new password if you have reason to believe that your password was accidentally disclosed to a third party.
- If the system notifies you that your password will expire soon or has expired, choose a new one as instructed. Contact your administrator in case of difficulty.

A RECOMMENDED method of generating passwords that fits these criteria while still being easy to memorize is to base it on letters of words in a sentence (NOT a famous quotation), including capitalization and punctuation and one or two variations. Example:

```
"Ask not for whom the bell tolls."
=> An4wtbt.

"Password 'P'9tw;ciSd' too weak; contained in SLES documentation"
=> P'9tw;ciSd
```

6.4 Access control for files and directories

Linux is a multiuser operating system. You can control which other users will be able to read or modify your files by setting the Unix permission bits and user/group IDs, or (if more precise control is needed) by using POSIX-style access control lists (ACLs).

Note that the administrators ('root') are able to override these permissions and access all files on the system. Use of encryption is RECOMMENDED for additional protection of sensitive data.

The 'umask' setting controls the permissions of newly created files and directories and specifies the access bits that will be *removed* from new objects. Ensure that the setting is appropriate, and never grant write access to others by default. The umask MUST include at least the 002 bit (no write access for others), and the RECOMMENDED setting is 027 (read-only and execute access for the group, no access at all for others).

Do not set up world-writable areas in the filesystem - if you want to share files in a controlled manner with a fixed group of other users (i.e. a project group), please contact your administrator and request the creation of a user group for that purpose.

Always remember that **you** are responsible for the security of the data you create and use. Choose permissions that match the protection goals appropriate for the content, and that correspond to your organization's security policy. Access to confidential data MUST be on a need-to-know basis, therefore do not make data world-readable unless the information is intended to be public.

Whenever you start a program or script, it will execute with your access rights. This implies that a malicious program would be able to read and modify all files that you have access to. Therefore, never execute any code that you have received from untrustworthy sources, and do not run commands that you do not understand.

Programs can be configured to run with the access rights of the program file's owner and/or group instead of the rights of the calling user. This is the setuid/setgid mechanism, which utilities such as *passwd*(1) use to be able to access security-critical files. You could also create your own setuid/setgid programs via *chmod*(1), but DO NOT do that unless you fully understand the security implications - you would be giving away *your* access privileges to whoever launches the setuid program. Please refer to the "Secure Programming HOWTO" in the unlikely case that you need to create such a program, there you will find explanations of the many aspects that must be considered, such as the risk of unintended shell escapes, buffer overflows, resource exhaustion attacks and many other factors.

Please refer to the *chmod*(1), *umask*(2), *chown*(1), *chgrp*(1), *acl*(5), *getfacl*(1), and *setfacl*(1) manual pages for information, or any of the many available books covering Linux security (cf. Appendix 'Literature'), or ask your system administrator for advice.

6.5 Data import / export

The system comes with various tools to archive data (*tar*, *star*, *cpio*). If ACLs are used, then only *star* MUST be used to handle the files and directories as the other commands do not support ACLs. The options *-H=exustar -acl* must be used with *star*.

Please see *star*(1) for more information.

7 Appendix

7.1 Online Documentation

If there are conflicting recommendations in this document and in one of the sources listed here, the Security Guide has precedence concerning the evaluated configuration.

Suse Linux Enterprise Server Security Guide *[this document]*, */usr/share/doc/packages/certification-sles-eal3/SLES-Security-Guide.**

SuSE Linux Enterprise Server Installation Guide, */usr/share/doc/packages/sles-inst-x86+x86-64_en/*

SuSE Linux Enterprise Server Administrator Guide, */usr/share/doc/packages/sles-admin-x86+x86-64_en/*

David A. Wheeler, "Secure Programming for Linux and Unix HOWTO", */usr/share/doc/howto/en/html_single/Secure-Programs-HOWTO.html*, *http://tldp.org/HOWTO/Secure-Programs-HOWTO/*

Kevin Fenzi, Dave Wreski, "Linux Security HOWTO", */usr/share/doc/howto/en/html_single/Security-HOWTO.html*, *http://www.linuxsecurity.com/docs/LDP/Security-HOWTO/*

7.2 Literature

Ellen Siever, Stephen Spainhour, Stephen Figgins, & Jessica P. Hekman, "Linux in a Nutshell, 3rd Edition", O'Reilly 2000, ISBN 0596000251

Simson Garfinkel, Gene Spafford, Alan Schwartz, "Practical Unix & Internet Security, 3rd Edition", O'Reilly 2003, ISBN 0596003234

leen Frisch, "Essential System Administration, 3rd Edition", O'Reilly 2002, ISBN 0596003439

Daniel J. Barrett, Richard Silverman, "SSH, The Secure Shell: The Definitive Guide", O'Reilly 2001, ISBN 0596000111

David N. Blank-Edelman, "Perl for System Administration", O'Reilly 2000, ISBN 1565926099

Shelley Powers, Jerry Peek, Tim O'Reilly, Mike Loukides, "Unix Power Tools, 3rd Edition", O'Reilly 2002, ISBN 0596003307

W. Richard Stevens, ”Advanced Programming in the UNIX(R) Environment”, Addison-Wesley 1992, ISBN 0201563177

Linda Mui, ”When You Can’t Find Your UNIX System Administrator”, O’Reilly 1995, ISBN 1565921046

7.3 The script `/usr/lib/eal3/bin/sles-eal3`

```
#!/bin/bash

usage () {
        echo "Usage: $0 [OPTIONS]"
        echo "    reconfigure system into EAL3 evaluated configuration"
        echo "Options:"
        echo "    -h|--help         show help"
        echo "    -i|--interactive  run interactively (default)"
        echo "    -a|--automated    run noninteractively"
        echo "    -v|--verbose      print detailed information while running"
}

args="$*"

base=/usr/lib/eal3
lib=$base/lib
funcs=$base/functions

LOGFILE=/var/log/certification-sles-eal3

# get all functions that this script needs:
for f in $funcs/*.sh; do
  . $f
done

# run various sanity checks before proceeding

if [ "‘/usr/bin/id -nu‘" != "root" ]; then
  die "This script must be run as root."
fi

if [ ! -f /proc/1/cmdline ]; then
  die "/proc is not mounted. Running a test?"
fi

if mount | grep ’ / ’ | grep "type ext3.*,acl" >/dev/null; then :; else
  die "root filesystem must be ext3 with ACL support on. See SG."
fi

if mount | grep "type nfs"; then
  die "please unmount all NFS shares first. See SG."
fi

if grep ’trusted:.*:.*:.’ /etc/group >/dev/null; then :; else
  die "No trusted users. You won’t be able to use ’su’. See SG."
fi
```

```
# special case to avoid a common cause of confusion - xinetd is not
# in the default install and people keep forgetting it.
#
if rpm -q xinetd >/dev/null 2>&1; then :; else
  die "You need to have xinetd installed to proceed. See SG."
fi

if ls -l /etc/init.d/audit-* 2>/dev/null; then
  log "You have leftover files from an obsolete version of this script."
  die "Remove /etc/init.d/audit-* before continuing."
fi

if ls -l /lib/liblaus.so* 2>/dev/null; then
  die "obsolete /lib/liblaus.so* found, please remove"
fi

# if the tests above were okay, let's proceed.

interactive="yes"
verbose=""

# commandline parsing
while [ ! -z "$1" ]; do
  case $1 in
    -h|--help)
        usage
        exit 0
        ;;
    -i|--interactive)
        interactive=yes
        shift
        ;;
    -a|--automated)
        interactive=""
        shift
        ;;
    -v|--verbose)
        verbose="yes"
        shift
        ;;
    *)
            usage
        exit 1
        ;;
  esac
done


# open logfile with first log:
logn "  ---  `date` script running: $0 args: $args"

if [ ! -z "$interactive" ]; then
        if [ ! -t 0 ]; then
                die "Interactive mode requested, but stdin is not a terminal"
```

```
        fi

        echo "You have chosen to run the reconfiguration in interactive mode."
        echo "The evaluated configuration requires that *all* the steps are"
        echo "done. If you want to do this automatically, stop and re-run the"
        echo "script in noninteractive mode (’-a’ option)."
        echo
        echo "The reconfiguration involves removing packages and modifying the"
        echo "system configuration, which may result in a system that is"
        echo "not useful to you. For example, the X11 desktop is removed."
        echo
        echo "Please read the documentation before proceeding."
        echo
        if ask "Continue?" "n"; then :; else
                die "Aborted. Your system was not modified."
        fi
fi

# bootloader configuration: grub needs no action, but if lilo is installed...
. /etc/sysconfig/bootloader
case "$LOADER_TYPE" in
  *lilo*)
        log "Your system uses lilo to load the kernel on system startup."
        log "The evaluated configuration does not support lilo as bootloader."
        log "It is necessary that you install the grub bootloader and configure"
        log "it so that your system will boot safely. The lilo bootloader will"
        log "either be removed automatically during the further processing of"
        log "this script, or you remove the package yourself (rpm -e lilo)"
        die "The script stops here."
        ;;
    *)
        ;;
esac



# rebuild the rpm database first before touching any packages:
if confirm "Running rpm --rebuilddb before package removal."; then
    rpm --rebuilddb
else
    log "rpm --rebuilddb was aborted."
fi


# package removal first.
ALLINSTALLEDPACKAGES=‘rpm -qa --queryformat=’%{NAME}\n’‘
logn "installed packages on the system: $ALLINSTALLEDPACKAGES"

PREREQPACKAGES=‘cat $lib/packagelist.required‘
ALLCERTIFIEDPACKAGES=‘cat $lib/packagelist.eal3‘
ALLTOLERATEDPACKAGES=‘cat $lib/packagelist.tolerated‘
pack_to_be_removed=""   # reminder...

for packreq in $PREREQPACKAGES; do
```

```
  packisok=""
  for packinst in $ALLINSTALLEDPACKAGES; do
    if [ "$packinst" = "$packreq" ]; then
      packisok="$packinst"
    fi
  done
  if [ -z "$packisok" ]; then
    die "Required prerequisite package ’$packreq’ missing, aborting."
  fi
done

for packinst in $ALLINSTALLEDPACKAGES; do
  packisok=""
    for packeal3 in $ALLCERTIFIEDPACKAGES $ALLTOLERATEDPACKAGES; do
        if [ "$packeal3" = "$packinst" ]; then
            packisok="$packinst"
        fi
    done
  if [ -z "$packisok" ]; then
      pack_to_be_removed="$pack_to_be_removed $packinst"
  fi
done

pack_to_be_removed=‘echo $pack_to_be_removed‘
if [ ! -z "$pack_to_be_removed" ]; then
    log "I want to remove the following packages:"
    log "$pack_to_be_removed"

    if confirm "Removing these RPMs from the system."; then
      logn "running: rpm -e $pack_to_be_removed"
      rpm -e $pack_to_be_removed || die "rpm package removal was unsuccessful.\
      Please do it manually. You can find the list of packages to be removed in the logf
    else
      log "removal of packages has been aborted"
      failure=1
    fi
fi

# need the correct architecture - checking the ’glibc’ arch via rpm doesn’t
# work on ppc64, since it returns ’ppc’. Use plain ’arch’ which gets the right
# result. Determining compatible RPMs is done below.
arch=‘arch‘

installed_kernel=‘rpm -qf --queryformat=’%{NAME}\n’ /boot/vmlinuz | tail -1‘
if [ -z "$installed_kernel" ]; then
  # that didn’t work, plan B...
  # There’s not /boot/vmlinuz on iSeries.
  installed_kernel=‘rpm -qa --queryformat=’%{NAME}\n’ \
  | egrep ’^(k_|kernel)’ | egrep -v ’tools|source’ | tail -1‘
fi
[ -z "$installed_kernel" ] && die "Can’t figure out the installed kernel version. Giving
logn "installed kernel is: $installed_kernel"

AuditModule="$base/lib/kernel/modules/$arch/$installed_kernel/audit.o"
```

```
ModuleDest=‘rpm -ql $installed_kernel | grep audit.o | tail -1‘
if [ -f "$AuditModule" ]; then
  if confirm "Install updated audit kernel module."; then
    old $ModuleDest
    cp -v $AuditModule $ModuleDest || die "Can’t install audit.o module."
    log "If you rebuild the kernel, please apply the patches in $base/lib/kernel/."
  fi
else
  log "Updated kernel module $AuditModule not found - wrong architecture or version."
  log "If you build your own kernel, please apply the patches in $base/lib/kernel/."
fi

# package installation:
# Get all files compatible with the architecture from the rpm directory

case "$arch" in
i386)
        archpacks=$base/rpm/*i386.rpm
        ;;
i486)
        archpacks=$base/rpm/*i[34]86.rpm
        ;;
i586)
        archpacks=$base/rpm/*i[345]86.rpm
        ;;
i686)
        archpacks=$base/rpm/*i[3456]86.rpm
        ;;
*)
        archpacks=$base/rpm/*$arch.rpm
        ;;
esac

# Install the packages, and check for any that need special handling.

for pack in $archpacks; do
  [ ! -f "$pack" ] && break

  name_of_package=‘rpm -qp --queryformat=’%{NAME}\n’ $pack‘
  logn "running: rpm --checksig $pack (package name: $name_of_package)"
  rpm --checksig $pack > /dev/null 2>&1
  if [ "$?" = 0 ]; then
    logn "  $pack sigcheck ok"
    case "$name_of_package" in
        k_*)
            if [ "$name_of_package" = "$installed_kernel" ]; then
                packstoinstall="$packstoinstall $pack"
            fi
            ;;
        glibc*)
            die "glibc upgrade not supported. Use service pack to do that."
            ;;
        *)
            packstoinstall="$packstoinstall $pack"
```

```
            ;;
    esac
  else
    die "checksig: package signature check for package $pack failed."
  fi
done

if [ "$packstoinstall" ]; then
  log "I want to install all packages from $base/rpm."
  log "The list of packages is $packstoinstall"
  if confirm "Installing these packages."; then
    logn "running: rpm --oldpackage --force --nodeps -Uhv $packstoinstall"
    rpm --oldpackage --force --nodeps -Uhv $packstoinstall || die "rpm package installat
       Please do it manually. The package list can be found in $LOGFILE"
  else
    log "Installation of packages aborted."
    failure=1
  fi
fi



# runlevel link removal:
if confirm "Removing all runlevel links from /etc/init.d/rc3.d."; then
  ( cd /etc/init.d/rc3.d; rm -f * nosuchfileordirectory_dummy )
  log "all runlevel symlinks removed."
else
  log "Removal of runlevel symlinks aborted."
  failure=1
fi


PERMITTED_SERVICES=‘cat $base/lib/permitted_services‘
logn "permitted services: $PERMITTED_SERVICES"
if confirm "Making links in /etc/init.d/rc3.d for all allowed services."; then
  for service in $PERMITTED_SERVICES; do
    logn "insserv /etc/init.d/$service"
    insserv /etc/init.d/$service
  done
  log "new runlevel symlinks created."
else
  log "new runlevel symlink creation in /etc/init.d/rc3.d aborted."
  failure=1
fi


for file in ‘cd $base; find etc -type f‘; do
  if confirm "Replacing the file /$file."; then
    logn "running: replace $file"
    replace $file
  else
    log "replacement of file /$file aborted."
    failure=1
  fi
```

```
done

if confirm "Installing new and updated manpages."; then
  log "Replacing manpages from $base/man to system paths."
  cd $base/man
  find . -type f -print0 | xargs -0 tar cf - | (cd /usr/share/man ; \
        tar xfvvp -)
  logn "manpages replaced."
else
  log "Replacing of manpages from $base/man to system paths aborted."
  failure=1
fi



# permissions of files:

if confirm "Removing setuid/setgid bits from all files in the system."; then
    output=‘find / -type f \( -perm +4000 -o -perm +2000 \) -print0 | \
        xargs -0 chmod -v -s 2>&1‘
    log "$output"
else
    log "setuid/setgid bit removal aborted."
    failure=1
fi

if confirm "Setting permissions according to /etc/permissions.eal3."; then
    logn "running: chkstat -set /etc/permissions.eal3"
    chkstat -set /etc/permissions.eal3
    log "Permissions are set (/etc/permissions.eal3)"
else
    log "setuid and setgid bits setting aborted (/etc/permissions.eal3)"
    failure=1
fi




# default runlevel:
if confirm "Changing default runlevel to 3."; then
    logn "changing default runlevel to 3"
    awk ’/^id:.:initdefault:$/ {
                print "id:3:initdefault:"; next; }
            { print $0; }’ < /etc/inittab > /etc/inittab.new
    logn "running: old /etc/inittab"
    old /etc/inittab
    logn "running: mv /etc/inittab.new /etc/inittab"
    mv /etc/inittab.new /etc/inittab
else
    log "initdefault change to 3 aborted."
    failure=1
    bootfail=1
fi
```

```
if [ -x /sbin/zipl ]; then
        if confirm "Run 'zipl' to update the boot loader configuration?"; then
                zipl
        fi
fi

# finally:
if [ -z "$bootfail" -a -z "$failure" ]; then
    log "Reconfiguring the system to the evaluated configuration is complete."
    log "It is now necessary to reboot the system."
    if confirm "Rebooting the system."; then
        log "rebooting the system now. Sleeping for 10 seconds..."
        exec 42>&-        # close logfile...
        sleep 10
        logn "running: /sbin/init 6"
        /sbin/init 6
        echo "Waiting to be killed..."
        sleep 600
    else
        log "reboot aborted. Please note that the system must be rebooted for"
        log "the configuration to be complete."
        failure=1
    fi
fi
```

7.4 The file `/etc/permissions.eal3`

```
# /etc/permissions.eal3
#
# Copyright (c) 2001 SuSE GmbH Nuernberg, Germany.  All rights reserved.
#
# Author: Roman Drahtmueller <draht@suse.de>, 2003
#
#
# See /etc/permissions for general hints on how to use this file.
#
# This file is based on /etc/permissions.secure as shipped with SLES8.
# It has been adapted to the needs of the EAL3 evaluation which disables
# a few more SUID programs.
# It still contains a lot more definitions than the minimal package set
# for the EAL3 evaluation, but those don't hurt in here.
#

#
# Directories
#
# closed:
/usr/lib/ircd                           irc.root          700
# No games:
/var/X11R6/scores                       root.root        0750
/var/catman                             man.root          755
```

```
/var/cron                               root.root         700
/var/spool/cron                         root.root         700
/var/cron/tabs                          root.root         700
/var/spool/cron/tabs                    root.root         700
/var/lib/gdm                            gdm.shadow        750
/var/lib/xdm/authdir                    root.root         700
/var/lib/xdm/authdir/authfiles          root.root         700
/var/lock                               root.uucp         775
# closed; see "easy"
/var/man2html                           root.root        0755
# no lock files for emacs:
/var/state/emacs/lock                   root.trusted     1775
/var/state/xemacs/lock                  root.trusted     1775
/var/lib/xemacs/lock                    root.trusted     1775
/var/squid                              squid.root        755
/var/squid/cache                        squid.root        755
/var/squid/logs                         squid.root        755


#
# /etc
#
/etc/crontab                            root.root         600
/etc/exports                            root.root         600
/etc/fstab                              root.root         600
/etc/ftpaccess                          root.root         600
/etc/ftpconversions                     root.root         600
/etc/ftpusers                           root.root         600
/etc/HOSTNAME                           root.root         644
/etc/hosts                              root.root         644
# Changing the hosts_access(5) files causes trouble with services
# that do not run as root!
/etc/hosts.allow                        root.root         644
/etc/hosts.deny                         root.root         644
/etc/hosts.equiv                        root.root         644
/etc/hosts.lpd                          root.root         644
/etc/inetd.conf                         root.root         600
/etc/inittab                            root.root         600
/etc/issue                              root.root         600
/etc/issue.net                          root.root         600
/etc/ld.so.conf                         root.root         644
/etc/ld.so.cache                        root.root         644
/etc/login.defs                         root.root         600
/etc/motd                               root.root         644
/etc/mtab                               root.root         600
/etc/rmtab                              root.root         600
/etc/services                           root.root         644
# changing the global ssh client configuration makes it unreadable
# and therefore useless. Keep in mind that users can bring their own client!
/etc/ssh_config                         root.root         644
/etc/sshd_config                        root.root         640
/etc/ssh_host_key.pub                   root.root         644
/etc/ssh_host_key                       root.root         600
/etc/ssh_random_seed                    root.root         600
```

```
/etc/ssh_known_hosts                    root.root         644
/etc/ssh/ssh_host_key                   root.root         600
/etc/ssh/ssh_host_key.pub               root.root         644
/etc/ssh/ssh_random_seed                root.root         600
/etc/ssh/ssh_config                     root.root         644
/etc/ssh/sshd_config                    root.root         640
/etc/syslog.conf                        root.root         600
/etc/termcap                            root.root         644

# sysconfig files:
/etc/sysconfig/network/providers        root.root         700


#
# suid system programs that need the suid bit to work:
#
/bin/su                                 root.trusted     4750
/usr/bin/su1                            root.root        0711
# disable at and cron for non-root users
/usr/bin/at                             root.trusted     4755
/usr/bin/crontab                        root.trusted     4755
/usr/bin/gpasswd                        root.trusted     4755
/usr/bin/newgrp                         root.root        0755
/usr/bin/passwd                         root.shadow      4755
/usr/bin/chfn                           root.shadow      4755
/usr/bin/chage                          root.shadow      4755
/usr/bin/chsh                           root.shadow      4755
/usr/bin/expiry                         root.shadow      0755
# NIS+: "trusted" only.
/usr/bin/chkey                          root.trusted     0755
# the default configuration of the sudo package in SuSE distribution is to
# intimidate users.
/usr/bin/sudo                           root.root        0755
/usr/sbin/suexec                        root.root        0755
/usr/sbin/su-wrapper                    root.root        0755
# opie password system
/etc/opiekeys                           root.root         600
/usr/bin/opiepasswd                     root.root        0755
/usr/bin/opiesu                         root.root        0755
# "user" entries in /etc/fstab make mount work for non-root users:
/usr/bin/ncpmount                       root.trusted     0755
/usr/bin/ncpumount                      root.trusted     0755
# mount/umount have had their problems already:
/bin/mount                              root.root        0755
/bin/umount                             root.root        0755
/usr/bin/fdmount                        root.root        0755
/usr/bin/ziptool                        root.trusted     0755
/bin/eject                              root.audio       0755
# sendmail calls the wrapper as daemon.daemon:
/usr/lib/majordomo/wrapper              root.daemon      0755
# glibc backwards compatibility
/usr/lib/pt_chown                       root.root        0755
/usr/lib64/pt_chown                     root.root        0755
/sbin/pwdb_chkpwd                       root.shadow      0755
```

```
/sbin/unix_chkpwd                       root.shadow      0755
/sbin/unix2_chkpwd                      root.shadow      0755
# qpopper
/usr/sbin/popauth                       pop.root         0755
# from the squid package
/usr/sbin/pam_auth                      root.shadow      0755

# utempter: See bottom of /etc/permissions:
/usr/sbin/utempter                      root.tty         2755


#
# log files that do not grow remarkably
#
/var/log/faillog                        root.root         600
/var/log/lastlog                        root.tty          644


#
# mixed section: most of it is disabled in this permissions.secure:
#
##############################################################################
# rpm subsystem:
/usr/src/packages/SOURCES               root.root         700
/usr/src/packages/BUILD                 root.root         700
/usr/src/packages/RPMS                  root.root         700
/usr/src/packages/RPMS/alpha            root.root         700
/usr/src/packages/RPMS/alphaev56        root.root         700
/usr/src/packages/RPMS/alphaev67        root.root         700
/usr/src/packages/RPMS/alphaev6         root.root         700
/usr/src/packages/RPMS/arm4l            root.root         700
/usr/src/packages/RPMS/athlon           root.root         700
/usr/src/packages/RPMS/i386             root.root         700
/usr/src/packages/RPMS/i486             root.root         700
/usr/src/packages/RPMS/i586             root.root         700
/usr/src/packages/RPMS/i686             root.root         700
/usr/src/packages/RPMS/ia64             root.root         700
/usr/src/packages/RPMS/mips             root.root         700
/usr/src/packages/RPMS/ppc              root.root         700
/usr/src/packages/RPMS/ppc64            root.root         700
/usr/src/packages/RPMS/powerpc          root.root         700
/usr/src/packages/RPMS/powerpc64        root.root         700
/usr/src/packages/RPMS/s390             root.root         700
/usr/src/packages/RPMS/s390x            root.root         700
/usr/src/packages/RPMS/sparc            root.root         700
/usr/src/packages/RPMS/sparcv9          root.root         700
/usr/src/packages/RPMS/sparc64          root.root         700
/usr/src/packages/RPMS/x86_64           root.root         700
/usr/src/packages/RPMS/mips             root.root         700
/usr/src/packages/RPMS/armv4l           root.root         700
/usr/src/packages/RPMS/noarch           root.root         700
/usr/src/packages/SPECS                 root.root         700
/usr/src/packages/SRPMS                 root.root         700
#
```

```
# mostly from series beo:
# see customs(8), export(1) and pmake(1)
/usr/bin/pmake                          root.root       0755
/usr/bin/export                         root.root       0755
/usr/bin/make                           root.root       0755
# Portable Batch System (PBS) (beo)
/usr/sbin/pbs_rcp                       root.root       0755
/usr/sbin/pbs_iff                       root.root       0755
# queue (beo)
/usr/bin/queue                          root.root       0755
# clusterit (beo)
/usr/bin/dsh                            root.root       0755
# dqs:
/usr/bin/qmod                           root.root       0755
/usr/bin/dqs_options                    root.root       0755
/usr/bin/qconf                          root.root       0755
# wants root for realtime scheduling policy class
# we better let it complain - on an idle machine it has no effect anyway.
/opt/rtsynth/RTSynth                    root.root       0755
# same here: package muse
/usr/bin/muse                           root.root       0755
# AX.25, NETROM, ROSE and TCP node frontend
/usr/sbin/node                          root.root       0755
##############################################################################
# executor, Mac-simulator:
/opt/executor/bin/executor-demo-svga    root.root       0755
# Amiga-emulator
/usr/bin/suae                           root.root       0755
# stonx: atari emulator, svgalib:
/usr/bin/sstonx                         root.root       0755
# atari800 emulator
/usr/bin/atari800                       root.root       0755
# z81 emulator
/usr/bin/z81txt                         root.root       0511
# package adamem (Z80 based ColecoVision and ColecoADAM emulator)
/usr/X11R6/lib/adamem/cvem              root.root       0755
/usr/X11R6/lib/adamem/adamem            root.root       0755
# video
/usr/X11R6/bin/v4l-conf                 root.video      0755
/opt/gnome/bin/zapping_setup_fb         root.video      0755
# vmware
/usr/bin/vmware.bin                     root.trusted    0755
/usr/bin/vmware-ping                    root.root       0755
# iBCS2 binary emulator
/shlib/protlib_s.emu                    root.root        755
/shlib/protlib_s.debug                  root.root        755
/shlib/libnsl_s.emu                     root.root        755
/shlib/libnsl_s.debug                   root.root        755
##############################################################################
# netatalk printer daemon:
/usr/sbin/papd                          root.lp         0755
# package cysched:
/opt/synchronize/linux/bin/synchrod     root.root       0755
/opt/synchronize/linux/bin/websyncd     root.root       0755
```

```
# scotty:
/usr/bin/ntping                         root.trusted    0755
/usr/bin/straps                         root.trusted    0755
/sbin/cardctl                           root.trusted    0755
# use it as root if you must:
/usr/X11R6/bin/dga                      root.root       0755
# screen savers:
# xlock and xlockmore have helper programs that do this job now:
/usr/X11R6/bin/xlock                    root.root       0755
/usr/X11R6/bin/xlock-mesa               root.root       0755
/usr/X11R6/bin/xscreensaver             root.root       0755
# This is not extensively tested.
/usr/bin/vlock                          root.shadow     0755
/usr/X11R6/bin/XFree86                  root.root       0711
/usr/X11R6/bin/Xwrapper                 root.root       0755
/usr/X11R6/bin/xemacs                   root.root       0755
/usr/bin/emacs                          root.root       0755
/usr/bin/man                            root.root       0755
/usr/bin/mandb                          root.root       0755
# turned off write and wall by disabling sgid tty:
/usr/bin/wall                          root.tty         0755
/usr/bin/write                         root.tty         0755
# linked against svgalib. Make it suid root if you want users to be
# able to use xaos on the console or keep it safe as this:
/usr/bin/xaos                          root.root        0755
# needs suid root for console font switches:
/usr/bin/kon.bin                        root.trusted    0755
# thttpd: sgid + executeable only for group www. Useless...
/usr/bin/makeweb                        root.www        2750
# ham series, package wampes: Disabled suid root
/usr/bin/bbs                            root.root       0755
# ham series, package dpbox
/usr/bin/dpgate                         dpbox.localham  0755
# sane package: disabled suid root.
/usr/bin/as6edriver                     root.root       0755
# yaps, pager software, accesses /dev/ttyS? . Disabled sgid uucp.
/usr/bin/yaps                           root.uucp       0755
# ncpfs tool: trusted only
/usr/bin/nwsfind                        root.trusted    0750
/usr/bin/ncplogin                       root.trusted    0750
/usr/bin/ncpmap                         root.trusted    0750
# dvisvga package: disabled suid root (for libvga)
/usr/bin/dvisvga                        root.root       0755
# maildrop package: change the permissions to the default from the
# rpm package (0755) if you have to use it. Default to deliver mails
# on a SuSE system is procmail.
/usr/bin/maildrop                       root.mail       0755
/usr/bin/dotlock                        root.mail       0755
# video editor. package mainactr, series pay
/opt/MainActor/MainActor                root.root       0755
/opt/MainActor/MainView                 root.root       0755
# conferencing system: some buffer overflows in there...
/usr/bin/bayonne_wrapper                root.root        755
# lpdfilter
```

```
/usr/lib/lpdfilter/bin/runlpr           root.root       0755
# disabled by default in SuSE distributions: make it 4755 if you need it.
/usr/bin/suidperl                       root.root       0755
# also disabled (libforms, libX11) reenable it by setting it 4755:
/usr/X11R6/bin/cardinfo                 root.root       0755
# if smail is installed:
/usr/sbin/smail                         root.root       0555
# phoenix, commercial package
# The package won't work with these files closed.
/usr/lib/phoenix/License                root.root        644
/usr/lib/phoenix/basic/address.txt      root.root        644
# apcupsd shouldn't need suid root
/sbin/apcupsd                           root.root        755
/usr/sbin/apcupsd                       root.root        755
# gnokii nokia cellphone software
/usr/sbin/mgnokiidev                    root.uucp        755
# plptools, palm pilot connectivity
/usr/sbin/plpnfsd                       root.trusted    0750
# pcp, performance co-pilot
/usr/share/pcp/bin/pmpost               root.trusted    0755
# mailman mailing list software
/usr/lib/mailman/cgi-bin/admin          root.mailman    0755
/usr/lib/mailman/cgi-bin/admindb        root.mailman    0755
/usr/lib/mailman/cgi-bin/archives       root.mailman    0755
/usr/lib/mailman/cgi-bin/edithtml       root.mailman    0755
/usr/lib/mailman/cgi-bin/handle_opts    root.mailman    0755
/usr/lib/mailman/cgi-bin/listinfo       root.mailman    0755
/usr/lib/mailman/cgi-bin/options        root.mailman    0755
/usr/lib/mailman/cgi-bin/private        root.mailman    0755
/usr/lib/mailman/cgi-bin/roster         root.mailman    0755
/usr/lib/mailman/cgi-bin/subscribe      root.mailman    0755
/usr/lib/mailman/mail/wrapper           root.mailman    0755
# apache frontpage extensions, disabled in secure and paranoid
/usr/lib/frontpage/version4.0/apache-fp/_vti_bin/fpexe root.root 0755
/usr/sbin/fpexec                        root.root       0755
/usr/sbin/validate                      root.root       0755
# sapdb; setuid root in permissions.easy
/opt/sapdb/depend/pgm/dbmsrv            root.root       0755
/opt/sapdb/depend/pgm/lserver           root.root       0755




#
# networking (need root for the privileged socket)
#
/bin/ping                               root.root       4755
/bin/ping6                              root.root       0755
/usr/bin/bing                           root.trusted    0755
# new traceroute program by Olaf Kirch does not need setuid root any more.
/usr/sbin/traceroute                    root.root       0755
/usr/sbin/traceroute6                    root.root       0755
# mtr is linked against ncurses.
/usr/sbin/mtr                           root.dialout    0755
```

```
/usr/bin/rcp                            root.root       0755
/usr/bin/rlogin                         root.root       0755
/usr/bin/rsh                            root.root       0755
# ssh is not suid here any more. If a user needs the rsh fallback feature,
# she should use /usr/bin/rsh.
/usr/bin/ssh                            root.root       0755
# ham radio
/var/mtrack/locfile                     root.root       0644
/var/mtrack/satfile                     root.root       0644
/usr/bin/kamplus                        root.localham   0750
/usr/bin/endhost                        root.localham   0750
/etc/kamrc                              root.localham    664
/var/lib/kamplus                        root.localham    775
/var/lib/kamplus/parms                  root.localham    775
/var/lib/kamplus/cq                     root.localham    664
/var/lib/kamplus/messages               root.localham    664
/var/lib/kamplus/helpfile-qt            root.localham    664
/var/lib/kamplus/capture.txt            root.localham    664
/var/lib/kamplus/parms/tnc.parms        root.localham    664
/var/lib/kamplus/parms/home             root.localham    664
/var/lib/kamplus/parms/away             root.localham    664
/usr/bin/kam-qt                         root.localham    750



#
# dialup networking programs
#
/usr/sbin/dip                           root.dialout    0755
/usr/sbin/pppd                          root.dialout    0750
/usr/sbin/cinternet-wwwrun              wwwrun.dialout  0750
/usr/sbin/pppoe-wrapper                 root.dialout    0750
/var/run/smpppd                         root.dialout     750
/var/lib/smpppd                         root.root        700
/etc/ppp                                root.dialout     750
/etc/ppp/chap-secrets                   root.root        600
/etc/ppp/pap-secrets                    root.root        600
/etc/pppoed.conf                        root.root        600
/etc/smpppd.conf                        root.root        600
/etc/smpppd-c.conf                      root.dialout     640
# i4l package:
/usr/sbin/isdnctrl                      root.uucp       0750
/usr/sbin/isdnbutton                     root.trusted   0755
/usr/bin/vboxbeep                        root.trusted   0755


#
# linux text console utilities
# since svgalib has vanished, only the mc cons.saver is left.
#
/usr/lib/mc/bin/cons.saver              root.root       0755


#
```

```
# terminal emulators
# This and future SuSE products have support for the utempter, a small helper
# program that does the utmp/wtmp update work with the necessary rights.
# The use of utempter obsoletes the need for sgid bits on terminal emulator
# binaries. We mention screen here, but all other terminal emulators have
# moved to /etc/permissions, with modes set to 0755.

# screen. multi-user mode needs suid root (4755). discouraged...
/usr/bin/screen                         root.root       0755

# this still uses the old /dev/ttypX terminal files. Needs
# suid root to chown the tty. Should do without, too.
/usr/X11R6/bin/xwawi                    root.tty        0755
# same here:
/usr/X11R6/bin/c16term                  root.tty        0755
# framebuffer terminal emulator (japanese). Most scary... Compare modes
# in "easy".
/usr/bin/jfbterm                        root.tty        0755
/usr/bin/newvc                          root.root       0755
/usr/bin/fld                            root.root       0755

#
# former suid programs
#
/usr/X11R6/bin/seyon                    root.uucp       0755
/usr/X11R6/bin/SuperProbe               root.root        755
/usr/X11R6/bin/XBF_NeoMagic             root.root        755
/usr/X11R6/bin/XF86_8514                root.root        755
/usr/X11R6/bin/XF86_AGX                 root.root        755
/usr/X11R6/bin/XF86_I128                root.root        755
/usr/X11R6/bin/XF86_Mach32              root.root        755
/usr/X11R6/bin/XF86_Mach64              root.root        755
/usr/X11R6/bin/XF86_Mach8               root.root        755
/usr/X11R6/bin/XF86_Mono                root.root        755
/usr/X11R6/bin/XF86_P9000               root.root        755
/usr/X11R6/bin/XF86_S3                  root.root        755
/usr/X11R6/bin/XF86_S3V                 root.root        755
/usr/X11R6/bin/XF86_SVGA                root.root        755
/usr/X11R6/bin/XF86_VGA16               root.root        755
/usr/X11R6/bin/XF86_W32                 root.root        755
/usr/X11R6/bin/XFCom_3DLabs             root.root        755
/usr/X11R6/bin/XFCom_Cyrix              root.root        755
/usr/X11R6/bin/XFCom_Rendition          root.root        755
/usr/X11R6/bin/XFCom_SiS                root.root        755
/usr/X11R6/bin/XSuSE_AT3D               root.root        755
/usr/X11R6/bin/XSuSE_Elsa_GLoria        root.root        755
/usr/X11R6/bin/XSuSE_Matrox             root.root        755
/usr/X11R6/bin/XSuSE_NVidia             root.root        755
/usr/X11R6/bin/XSuSE_Tseng              root.root        755
/usr/X11R6/bin/xcpustate                root.root        755
/usr/X11R6/bin/xload                    root.root        755
/usr/X11R6/bin/xosview.bin              root.root        755
/usr/X11R6/bin/xosview                  root.root        755
/usr/bin/cu                             root.root        755
```

```
/usr/bin/cdrecord                       root.root       755
/usr/bin/elm                            root.root       755
/usr/bin/filter                         root.root       755
/usr/bin/deliver                        root.root       755
/usr/bin/lockfile                       root.root       755
/usr/bin/minicom                        root.uucp       755
/usr/bin/mutt                           root.root       755
/usr/bin/procmail                       root.root       755
/usr/sbin/atrun                         root.root       755
/usr/bin/mh/inc                         root.root       755
/usr/bin/mh/msgchk                      root.root       755


#
# kde+kde2
# (all of them are disabled in permissions.secure except for
# the helper programs)
#
# arts wrapper, normally suid root:
/opt/kde3/bin/artswrapper               root.root       0755
/opt/kde2/bin/artswrapper               root.root       0755
# set this to suid root (4755) if you're running shadow via NIS:
/opt/kde3/bin/kcheckpass                root.shadow     0755
# getting group id disk means root. See modes of disk device files!
/opt/kde3/bin/kscd                      root.disk       0755
# This has a meaning:
/opt/kde3/bin/kdesud                    root.nogroup    2755
/opt/kde2/bin/kdesud                    root.nogroup    2755
# devpts obsoletes this:
/opt/kde3/bin/konsole_grantpty          root.root       0755
/opt/kde2/bin/konsole_grantpty          root.root       0755
/opt/kde3/bin/kreatecd_rootwrapper      root.root       0755
/opt/kde2/bin/kpac_dhcp_helper          root.root       0755
/opt/kde3/bin/kpac_dhcp_helper          root.root       0755
/opt/kde2/bin/kradio                    root.video      0755
/opt/kde2/bin/kwintv                    root.video      0755
# kdemultimedia3-sound, gift
/var/cache/gift                         root.root       0755
/var/cache/cddb                         root.root       0755
/var/cache/cddb/blues                   root.root       0755
/var/cache/cddb/classical               root.root       0755
/var/cache/cddb/country                 root.root       0755
/var/cache/cddb/data                    root.root       0755
/var/cache/cddb/folk                    root.root       0755
/var/cache/cddb/jazz                    root.root       0755
/var/cache/cddb/misc                    root.root       0755
/var/cache/cddb/newage                  root.root       0755
/var/cache/cddb/reggae                  root.root       0755
/var/cache/cddb/rock                    root.root       0755
/var/cache/cddb/soundtrack              root.root       0755



# xmcd database, open only in permissions.easy
```

```
/var/lib/xmcd/discog                    root.root        755
/var/lib/xmcd/discog/Blues              root.root        755
/var/lib/xmcd/discog/Blues/General_Blues/index.html root.root       644
/var/lib/xmcd/discog/Classical          root.root        755
/var/lib/xmcd/discog/Classical/General_Classical/index.html root.root 644
/var/lib/xmcd/discog/Country            root.root        755
/var/lib/xmcd/discog/Country/General_Country/index.html root.root   644
/var/lib/xmcd/discog/Data               root.root        755
/var/lib/xmcd/discog/Data/General_Data/index.html  root.root        644
/var/lib/xmcd/discog/Folk               root.root        755
/var/lib/xmcd/discog/Folk/General_Folk/index.html  root.root        644
/var/lib/xmcd/discog/Jazz               root.root        755
/var/lib/xmcd/discog/Jazz/General_Jazz/index.html  root.root        644
/var/lib/xmcd/discog/Newage             root.root        755
/var/lib/xmcd/discog/Newage/General_Newage/index.html root.root     644
/var/lib/xmcd/discog/Rock               root.root        755
/var/lib/xmcd/discog/Rock/General_Rock/index.html  root.root        644
/var/lib/xmcd/discog/Soundtrack         root.root        755
/var/lib/xmcd/discog/Soundtrack/General_Soundtrack/index.html root.root 644
/var/lib/xmcd/discog/Unclassifiable     root.root        755
/var/lib/xmcd/discog/Unclassifiable/General_Unclassifiable/index.html root.root 644
/var/lib/xmcd/discog/World              root.root        755
/var/lib/xmcd/discog/World/Reggae       root.root        755
/var/lib/xmcd/discog/World/Reggae/index.html       root.root        644
/var/lib/xmcd/discog/index.html         root.root        644
```

```
#
# amanda
#
# Well, if you are gid disk already, you don't need these amanda binaries
# to get root.
# Anyway, we don't keep the suid bits.
/usr/sbin/amcheck                       root.disk       0750
/usr/lib/amanda/calcsize                root.disk       0750
/usr/lib/amanda/rundump                 root.disk       0750
/usr/lib/amanda/planner                 root.disk       0750
/usr/lib/amanda/runtar                  root.disk       0750
/usr/lib/amanda/dumper                  root.disk       0750
/usr/lib/amanda/killpgrp                root.disk       0750


#
# ingres
# all suid and sgid bits cleared.
/usr/ingres/bin                         root.root       0755
/usr/ingres/bin/creatdb                 root.root       0751
/usr/ingres/bin/destroydb               root.root       0751
/usr/ingres/bin/helpr                   root.root       0751
/usr/ingres/bin/ingconv                 root.root       0751
/usr/ingres/bin/ingres                  root.root       0751
```

```
/usr/ingres/bin/printadmin              root.root       0751
/usr/ingres/bin/printr                  root.root       0751
/usr/ingres/bin/purge                   root.root       0751
/usr/ingres/bin/restore                 root.root       0751
/usr/ingres/bin/sysdump                 root.root       0751
/usr/ingres/bin/sysmod                  root.root       0751
/usr/ingres/bin/sysmodfunc              root.root       0751
/usr/ingres/bin/univingres              root.root       0751
#   :-)
/usr/ingres/bin/usersetup               root.root       0700
/opt/tngfw/ingres/utility/csreport      ingres.sys      0755
/opt/tngfw/ingres/files/iipwd/ingvalidpw.dis ingres.sys 0755
/opt/tngfw/secu/bin/cadatefmt           root.root       0755
/opt/tngfw/cadb/system/cadb_sut         root.root       0755
/opt/tngfw/cadb/system/dbserver         root.sys        0755
/opt/tngfw/wv/bin/create_repository     root.root       0755
/opt/tngfw/wv/bin/fwrpt                 root.root       0755
/opt/tngfw/wv/bin/dscvrbe               root.root       0755
/opt/tngfw/wv/bin/carxwvdg              root.root       0755
/opt/tngfw/wv/bin/discwiz               root.root       0755
/opt/tngfw/wv/bin/tools_scripts         root.root       0755
/opt/tngfw/wv/bin/emrport               root.root       0755
/opt/tngfw/wv/bin/emrpt                 root.root       0755
/opt/tngfw/wv/bin/logonserver.exe       root.root       0755
/opt/tngfw/wv/bin/dscvrone              root.root       0755
/opt/tngfw/wv/bin/dscvrbe_stop          root.root       0755
/opt/tngfw/cal                          root.root        755

#
# yard
# all suid and sgid bits cleared.
/usr/lib/YARD/bin/yardarch              root.yard       0750
/usr/lib/YARD/bin/yardck                root.yard       0750
/usr/lib/YARD/bin/yardd                 root.yard       0750
/usr/lib/YARD/bin/yardflush             root.yard       0750
/usr/lib/YARD/bin/yardinit              root.yard       0750
/usr/lib/YARD/bin/yardlog               root.yard       0750
/usr/lib/YARD/bin/yardsrv               root.yard       0755
/usr/lib/YARD/bin/yardstat              root.yard       0755
/usr/lib/YARD/bin/yarduser              root.yard       0555


#
# gnats
#
/usr/lib/gnats/gen-index                gnats.root      4555
/usr/lib/gnats/pr-edit                  gnats.root      4555
/usr/lib/gnats/queue-pr                 gnats.root      4555


#
# news (inn)
#
# suid root bits cleared.
```

```
/usr/lib/news/bin/rnews                 news.uucp       0755
/usr/lib/news/bin/startinnfeed          root.news       0755
/usr/lib/news/bin/inndstart             root.news       0755
/usr/lib/news/bin/inews                 news.news       0755


#
# fax
#
# restrictive, only for "trusted" group users:
/var/spool/fax/outgoing                root.trusted     1770
/var/spool/fax/outgoing/locks          root.trusted     1770
/var/spool/fax/archive                  uucp.uucp        700
/var/spool/fax/bin                      uucp.uucp        755
/var/spool/fax/client                   uucp.uucp        755
/var/spool/fax/config                   uucp.uucp        755
/var/spool/fax/dev                      uucp.uucp        755
/var/spool/fax/docq                     uucp.uucp        700
/var/spool/fax/doneq                    uucp.uucp        700
/var/spool/fax/etc                      uucp.uucp        755
/var/spool/fax/info                     uucp.uucp        755
/var/spool/fax/log                      uucp.uucp        755
/var/spool/fax/pollq                    uucp.uucp        700
/var/spool/fax/recvq                    uucp.uucp        755
/var/spool/fax/sendq                    uucp.uucp        700
/var/spool/fax/status                   uucp.uucp        755
/var/spool/fax/tmp                      uucp.uucp        700


#
# tex
#
/var/texfonts/pk/deskjet                root.root       0775
/var/texfonts/pk/gsftopk                root.root       0775
/var/texfonts/pk                        root.root       0775
/var/texfonts                           root.root       0775


#
# uucp
#
/var/spool/uucppublic                   root.uucp       1770
/var/spool/uucp                         uucp.uucp        755
/usr/bin/uucp                           uucp.uucp       0555
/usr/bin/uuname                         uucp.uucp       0555
/usr/bin/uustat                         uucp.uucp       0555
/usr/bin/uux                            uucp.uucp       0555
/usr/lib/uucp/uucico                    uucp.uucp       0555
/usr/lib/uucp/uuxqt                     uucp.uucp       0555
/var/lib/uucp/taylor_config/call        uucp.uucp        440
/var/lib/uucp/taylor_config/passwd      uucp.uucp        440
/var/log/uucp                           uucp.uucp        755
```

```
#
# games of all kinds, toys
# all suid and sgid bits cleared.
#
# directories:
/var/games                              games.games     0775
/var/games/sasteroids                   games.games     0775
/var/games/xbl                          games.games     0775
/var/games/sail                         games.games     0775
/var/games/phantasia                    games.games     0775
/var/games/kugel-scorefile              games.games     0664
/var/games/kjewelscore                  games.games     0664
/var/games/xgalaga/scores               games.games     0664
/var/games/xsok                         games.games     0775
/var/games/xsok/Cyberbox.score          games.games     0664
/var/games/xsok/Sokoban.score           games.games     0664
/var/games/xsok/Xsok.score              games.games     0664
/var/games/xbill/scores                 games.games     0664
/var/games/geki2.scores                 games.games     0664
/var/games/grande.scores                games.games     0664


# svgalib:
/usr/games/abuse.console                root.root       0755
# SpaceBoom: not in SuSE-7.1 any more:
/usr/games/SpaceBoom/SpaceBoom          root.root       0755
/usr/games/synaesthesia                 root.root       0755
/usr/games/sasteroids                   root.games      0755
/usr/games/snake                        games.games     0755
/usr/games/wtf                          games.games     0755
/usr/games/trek                         games.games     0755
/usr/games/cribbage                     games.games     0755
/usr/games/arithmetic                   games.games     0755
/usr/games/quiz                         games.games     0755
/usr/games/backgammon                   games.games     0755
/usr/games/banner                       games.games     0755
/usr/games/canfield                     games.games     0755
/usr/games/wargames                     games.games     0755
/usr/games/fish                         games.games     0755
/usr/games/tetris-bsd                   games.games     0755
/usr/games/apxserver                    games.games     0755
/usr/games/huntd                        games.games     0755
/usr/games/hunt                         games.games     0755
/usr/games/rot13                        games.games     0755
/usr/games/boggle                       games.games     0755
/usr/games/pig                          games.games     0755
/usr/games/worms                        games.games     0755
/usr/games/robots                       games.games     0755
/usr/games/yahtzee                      games.games     0755
/usr/games/Maelstrom                    games.games     0755
/usr/games/monop                        games.games     0755
/usr/games/random                       games.games     0755
/usr/games/cfscores                     games.games     0755
/usr/games/number                       games.games     0755
```

```
/usr/games/mille                    games.games     0755
/usr/games/ppt                      games.games     0755
/usr/games/adventure                games.games     0755
/usr/games/morse                    games.games     0755
/usr/games/battlestar               games.games     0755
/usr/games/sail                     games.games     0755
/usr/games/rain                     games.games     0755
/usr/games/countmail                games.games     0755
/usr/games/factor                   games.games     0755
/usr/games/caesar                   games.games     0755
/usr/games/wump                     games.games     0755
/usr/games/snscore                  games.games     0755
/usr/games/gomoku                   games.games     0755
/usr/games/pom                      games.games     0755
/usr/games/bin/cfsndserv            games.games     0755
/usr/games/bin/cfclient             games.games     0755
/usr/games/bin/gcfclient            games.games     0755
/usr/games/bin/crossfire            games.games     0755
/usr/games/hangman                  games.games     0755
/usr/games/dm                       games.games     0755
/usr/games/atc                      games.games     0755
/usr/lib/nethack/nethack.gtk        games.games     0755
/usr/lib/nethack/nethack.tty        games.games     0755
/usr/lib/nethack/nethack.qt         games.games     0755
/usr/lib64/nethack/nethack.gtk        games.games     0755
/usr/lib64/nethack/nethack.tty        games.games     0755
/usr/lib64/nethack/nethack.qt         games.games     0755
# falconseye
/usr/lib/nethack/nethack.fe         games.games     0755
/usr/lib64/nethack/nethack.fe         games.games     0755
/usr/games/primes                   games.games     0755
/usr/games/phantasia                games.games     0755
/usr/games/bcd                      games.games     0755
/usr/games/worm                     games.games     0755
/usr/games/teachgammon              games.games     0755
/usr/games/chromium                 games.games     0755
/usr/games/crossfire                games.games     0755
/usr/games/geki2                    games.games     0755
/usr/games/grande                   games.games     0755
/usr/games/xscrab                   games.games     0755
/usr/bin/ltris                      games.games     0755
/usr/bin/xlogical                   games.games     0755
/usr/bin/lbreakout                  games.games     0755
/usr/bin/lbreakout2                 games.games     0755
# d1x descent
/usr/share/games/d1x/d1x143sh       games.games     0755
/usr/X11R6/bin/mirrormagic          games.games     0755
/usr/X11R6/bin/xboing               games.games     0755
/usr/X11R6/bin/xboingrp             games.games     0755
/usr/X11R6/bin/xbombs               games.games     0755
/usr/X11R6/bin/xgalaga              games.games     0755
/usr/X11R6/bin/tophextris           games.games     0755
/usr/X11R6/bin/xtetris              games.games     0755
/usr/X11R6/bin/xhextris             games.games     0755
```

```
/usr/X11R6/bin/cxhextris                games.games     0755
/usr/X11R6/bin/xdigger                  games.games     0755
/usr/X11R6/bin/xkobo                    games.games     0755
/usr/X11R6/bin/xmris                    games.games     0755
/usr/X11R6/bin/xbl                      games.games     0755
/usr/X11R6/bin/battalion                games.games     0755
/usr/X11R6/bin/rocksndiamonds           games.games     0755
# gnome-games
/opt/gnome2/bin/gtali                   games.games     0755
/opt/gnome2/bin/gnotski                 games.games     0755
/opt/gnome2/bin/gnome-stones            games.games     0755
/opt/gnome2/bin/glines                  games.games     0755
/opt/gnome2/bin/gnibbles                games.games     0755
/opt/gnome2/bin/iagno                   games.games     0755
/opt/gnome2/bin/gnotravex               games.games     0755
/opt/gnome/bin/sol                      games.games     0755
/opt/gnome/bin/gturing                  games.games     0755
/opt/gnome/bin/gnome-xbill              games.games     0755
/opt/gnome2/bin/mahjongg                games.games     0755
/opt/gnome2/bin/gnometris               games.games     0755
/opt/gnome/bin/ctali                    games.games     0755
/opt/gnome2/bin/gnobots2                games.games     0755
/opt/gnome2/bin/gnomine                 games.games     0755
/opt/gnome2/bin/same-gnome              games.games     0755
/opt/gnome/bin/freecell                 games.games     0755
/opt/gnome/bin/GnomeScott               games.games     0755
/opt/gnome/bin/gataxx                   games.games     0755
/opt/gnome/bin/soundtracker             root.root       0755
/opt/gnome/bin/gewels                   games.games     0755
/opt/gnome/bin/gnect                    games.games     0755

# lprng
# FIXME: setuid root is bad - setgid lp should be sufficient...
/usr/bin/lpq                                root.lp                 2755
/usr/bin/lpr                                root.lp                 2755
/usr/bin/lprm                                root.lp                 2755
/usr/bin/lpstat                         root.lp                 2755

#
# postfix
/usr/sbin/postdrop                        root.maildrop         2755
/usr/sbin/postqueue                        root.maildrop         2755

# Security configuration and old passwords
/etc/security                           root.root       0755
/etc/security/opasswd                   root.root       0600

/usr/lib/news                           root.root       0750
/etc/news                               root.root       0750
/etc/uucp                               root.root       0750

# Audit configuration and log files
/etc/audit                              root.root       0700
/etc/audit/audit.conf                   root.root       0600
```

```
/etc/audit/filter.conf                  root.root       0600
/etc/audit/eal3files.conf               root.root       0600
/var/log/audit                          root.root       0600
/var/log/audit.d                        root.root       0700
```

7.5 The file `/etc/init.d/audit`

```
#! /bin/sh
# Copyright (c) 2003 SuSE Linux AG, Nuernberg, Germany.
#
# Author: Olaf Kirch <okir@suse.de>
#
# /etc/init.d/audit
#
### BEGIN INIT INFO
# Provides: audit
# Required-Start:
# Required-Stop:
# Default-Start: 2 3 5
# Default-Stop: 0 1 6
# Description: Start audit subsystem
### END INIT INFO

# Set defaults and read admin preferences
AUDIT_ALLOW_SUSPEND=1
AUDIT_ATTACH_ALL=0
AUDIT_MAX_MESSAGES=1024
AUDIT_PARANOIA=0

test -s /etc/sysconfig/audit && \
      . /etc/sysconfig/audit

AUDITD_BIN=/sbin/auditd

# FIXME: use shell daemon and kill system on auditd failure ?!

# ppc special case - use 64-bit binary on ppc64
#
if [ ‘arch‘ = ’ppc64’ ];then
        AUDITD_BIN=/sbin/auditd64
fi

# ppc special case #2 - we may be running a 32bit shell (arch==ppc) on ppc64,
# but the auditd was launched from a 64bit shell (arch==ppc64). Fix up the
# binary name in that case (also for other 64-bit platforms)
#
if ps ax | grep -v grep | grep auditd64 >/dev/null; then
        AUDITD_BIN=/sbin/auditd64
fi

test -x $AUDITD_BIN || exit 5
```

```
# Shell functions sourced from /etc/rc.status:
#      rc_check         check and set local and overall rc status
#      rc_status        check and set local and overall rc status
#      rc_status -v     ditto but be verbose in local rc status
#      rc_status -v -r  ditto and clear the local rc status
#      rc_failed        set local and overall rc status to failed
#      rc_failed <num>  set local and overall rc status to <num><num>
#      rc_reset         clear local rc status (overall remains)
#      rc_exit          exit appropriate to overall rc status
. /etc/rc.status

# First reset status of this service
rc_reset

# Return values acc. to LSB for all commands but status:
# 0 - success
# 1 - generic or unspecified error
# 2 - invalid or excess argument(s)
# 3 - unimplemented feature (e.g. "reload")
# 4 - insufficient privilege
# 5 - program is not installed
# 6 - program is not configured
# 7 - program is not running
#
# Note that starting an already running service, stopping
# or restarting a not-running service as well as the restart
# with force-reload (in case signalling is not supported) are
# considered a success.

configure_module () {
        if /sbin/lsmod | grep audit >/dev/null; then :; else
                /sbin/modprobe audit 2>/dev/null
                sleep 1
        fi
        echo $AUDIT_ALLOW_SUSPEND > /proc/sys/dev/audit/allow-suspend
        echo $AUDIT_ATTACH_ALL > /proc/sys/dev/audit/attach-all
        echo $AUDIT_MAX_MESSAGES > /proc/sys/dev/audit/max-messages
        echo $AUDIT_PARANOIA > /proc/sys/dev/audit/paranoia
}

case "$1" in
    start)
        echo -n "Starting audit subsystem"
        ## Start daemon with startproc(8). If this fails
        ## the echo return value is set appropriate.
        configure_module
        /sbin/startproc $AUDITD_BIN || return=$rc_failed

        # give auditd some time to initialize, so that auditing
        # is active when the script is done.
        sleep 1

        # Remember status and be verbose
        rc_status -v
```

```
    ;;
inittab)
        # not intended for interactive use; this mode
    # is for running auditd from /etc/inittab, i.e.:
    #     au:35:/etc/init.d/audit inittab
    configure_module
        $AUDITD_BIN -F 2>>/var/log/auditd.log
    ;;
stop)
    echo -n "Shutting down audit subsystem"
    /sbin/killproc -TERM $AUDITD_BIN

    # Remember status and be verbose
    rc_status -v
    ;;
try-restart)
    ## Stop the service and if this succeeds (i.e. the
    ## service was running before), start it again.
    ## Note: try-restart is not (yet) part of LSB (as of 0.7.5)
    $0 status >/dev/null &&  $0 restart

    # Remember status and be quiet
    rc_status
    ;;
restart)
    ## If first returns OK call the second, if first or
    ## second command fails, set echo return value.
    $0 stop  &&  $0 start  ||  return=$rc_failed
    ;;
force-reload)
    ## Signal the daemon to reload its config. Most daemons
    ## do this on signal 1 (SIGHUP).
    ## If it does not support it, restart.

    echo -n "Reload audit configuration"
    configure_module
    killproc -HUP $AUDITD_BIN

    rc_status
    ;;
reload)
    echo -n "Reload audit configuration"
    configure_module
    killproc -HUP $AUDITD_BIN

    # If it supports signalling:
    #killproc -HUP $AUDITD_BIN
    #touch /var/run/FOO.pid
    #rc_status -v

    # Otherwise if it does not support reload:
    rc_failed 3
    rc_status -v
    ;;
```

```
    status)
        echo -n "Checking for audit daemon: "
        ## Check status with checkproc(8), if process is running
        ## checkproc will return with exit status 0.

        # Status has a slightly different for the status command:
        # 0 - service running
        # 1 - service dead, but /var/run/  pid  file exists
        # 2 - service dead, but /var/lock/ lock file exists
        # 3 - service not running

        # NOTE: checkproc returns LSB compliant status values.
        checkproc $AUDITD_BIN
        rc_status -v
        ;;
    *)
        echo "Usage: $0 {start|stop|status|try-restart|restart|force-reload|reload}"
        exit 1
esac
rc_exit
```

7.6 The file `/etc/audit/audit.conf`

```
# kernel interface
device-file = "/dev/audit";

# filter config
filter-config = "/etc/audit/filter.conf";

# Standard output method is bin mode.
#
output {
        mode                = bin;
        num-files        = 4;
        file-size        = 20M;
        file-name        = "/var/log/audit.d/bin";
        notify                = "/usr/sbin/audbin -S /var/log/audit.d/save.%u -C";

        # The following symlink is created whenever we switch to
        # a new bin.
        current                = "/var/log/audit";

        # force a disk flush after each record? This slows things
        # down greatly, but helps preserve records in case of a crash.
        sync                = no;

        error {
                action {
                        type = suspend;
                };
        };
};
```

```
# Alternatively, write to /var/log/audit in normal
# append mode
# output {
#        mode                = append;
#        file-name        = "/var/log/audit";
#        sync                = yes;
# };

# Alternative output
# output {
#        mode                = stream;
#        command                = "/usr/local/sbin/send_to_syslog"
# };

# Disk usage thresholds.
# These thresholds are checked at regular intervals when
# append mode is used.
# (bin mode doesn't require these checks as the bin files
# are preallocated).
threshold disk-space-low {
        space-left = 10M;
        action {
                type = syslog;
                facility = security;
                priority = warning;
        };
        action {
                type = notify;
                command = "/usr/local/bin/page-admin";
        };
        action {
                type = audit;
                event = AUDIT_disklow;
        };
};

threshold disk-full {
        space-left = 20K;
        action {
                type = syslog;
                facility = security;
                priority = crit;
        };
        action {
                type = audit;
                event = AUDIT_diskfull;
        };
};
```

7.7 The file `/etc/audit/filter.conf`

```
#
# This is a sample filter.conf file.
```

```
# Please take a look at filesets.conf first if you
# wish to customize what system calls will be logged.
#
# The syntax of this file is described in filter.conf(5).
#

#
# Various primitive predicates
predicate        is-null                = eq(0);
predicate        is-negative          = lt(0);
predicate        is-system-uid          = lt(100);
predicate        is-lower-1024          = lt(-1024);


#
# Predicate to check open(2) mode: true iff
# (mode & O_ACCMODE) == O_RDONLY
predicate        is-rdonly          = mask(O_ACCMODE, O_RDONLY);

#
# Predicates for testing file type, valid when applied
# to a file type argument
predicate        __isreg                = mask(S_IFMT, S_IFREG);
predicate        __isdir                = mask(S_IFMT, S_IFDIR);
predicate        __ischr                = mask(S_IFMT, S_IFCHR);
predicate        __isblk                = mask(S_IFMT, S_IFBLK);
predicate        __issock         = mask(S_IFMT, S_IFSOCK);
predicate        __islnk                = mask(S_IFMT, S_IFLNK);
predicate        s_isreg                = __isreg(file-mode);
predicate        s_isdir                = __isdir(file-mode);
predicate        s_ischr                = __ischr(file-mode);
predicate        s_isblk                = __isblk(file-mode);
predicate        s_issock         = __issock(file-mode);
predicate        s_islnk                = __islnk(file-mode);
predicate        is-tempdir          = mask(01777, 01777);
predicate        is-world-writable = mask(0666, 0666);

#
# Predicates dealing with process exit code
predicate        if-crash-signal        =
                       !mask(__WSIGMASK, 0)
                        && (mask(__WSIGMASK, __WSIGILL) ||
                            mask(__WSIGMASK, __WSIGABRT) ||
                            mask(__WSIGMASK, __WSIGSEGV) ||
                            mask(__WSIGMASK, __WSIGSTKFLT));

#
# Predicates for audit-tags
predicate        is-o-creat               = mask(O_CREAT, O_CREAT);
predicate        is-ipc-remove               = eq(IPC_RMID);
predicate        is-ipc-setperms               = eq(IPC_SET);
predicate        is-ipc-creat              = mask(IPC_CREAT, IPC_CREAT);
predicate        is-auditdevice               = prefix("/dev/audit");
predicate        is-cmd-set-auditid       = eq(AUIOCSETAUDITID);
```

```
predicate        is-cmd-set-loginid        = eq(AUIOCLOGIN);
predicate        is-audit-setfilter        = eq(113);
predicate       is-audit-log                = prefix("/var/log/audit.d");

#
# Misc filters
filter                is-root                       = is-null(uid);
filter                is-setuid                  = is-null(dumpable);
filter                syscall-failed                  = is-negative(result);
filter                syscall-addr-succeed         = is-lower-1024(result);
predicate        is-af-packet                = eq(AF_PACKET);
predicate        is-af-netlink                = eq(AF_NETLINK);
predicate        is-sock-raw                = eq(SOCK_RAW);

#
# Include filesets.
#
include "eal3files.conf";


#
# "Secret" files should not be read by everyone -
# we also log read access to these files
#
# predicate        is-secret = prefix(@secret-files);

#
# All regular files owned by a system uid are deemed sensitive
#
predicate        is-system-file = is-system-uid(file-uid)
                            && ! (prefix("/var") || prefix("/tmp"))
                            && !is-world-writable(file-mode);

#
# Define ioctls we track
#
set                sysconf-ioctls = {
        SIOCADDDLCI,
        SIOCADDMULTI,
        SIOCADDRT,
        SIOCBONDCHANGEACTIVE,
        SIOCBONDENSLAVE,
        SIOCBONDRELEASE,
        SIOCBONDSETHWADDR,
        SIOCDARP,
        SIOCDELDLCI,
        SIOCDELMULTI,
        SIOCDELRT,
        SIOCDIFADDR,
        SIOCDRARP,
        SIOCETHTOOL,
        SIOCGIFBR,
        SIOCSARP,
        SIOCSIFADDR,
```

```
        SIOCSIFBR,
        SIOCSIFBRDADDR,
        SIOCSIFDSTADDR,
        SIOCSIFENCAP,
        SIOCSIFFLAGS,
        SIOCSIFHWADDR,
        SIOCSIFHWBROADCAST,
        SIOCSIFLINK,
        SIOCSIFMAP,
        SIOCSIFMEM,
        SIOCSIFMETRIC,
        SIOCSIFMTU,
        SIOCSIFNAME,
        SIOCSIFNETMASK,
        SIOCSIFPFLAGS,
        SIOCSIFSLAVE,
        SIOCSIFTXQLEN,
        SIOCSMIIREG
};
predicate is-sysconf-ioctl        = eq(@sysconf-ioctls);

#
# System calls on file names
#
set        file-ops = {
                        "mkdir", "rmdir", "unlink",
                        "chmod",
                               "chown", "lchown",
                        "chown32", "lchown32",
};

#
# General system related ops
#
set        system-ops = {
                        swapon, swapoff,
                        create_module, init_module, delete_module,
                        sethostname, setdomainname,
};

set        priv-ops = {
                        "setuid",
                        "setuid32",
                        "seteuid",
                        "seteuid32",
                        "setreuid",
                        "setreuid32",
                        "setresuid",
                        "setresuid32",
                        "setgid",
                        "setgid32",
                        "setegid",
                        "setegid32",
                        "setregid",
```

```
                        "setregid32",
                        "setresgid",
                        "setresgid32",
                        "setgroups",
                        "setgroups32",
                        "capset",
};

#
# Audit-Tags (only syscall related tags are handled here)
#

# define sets of syscalls related to audit-tags

# System calls for changing file modes
set        mode-ops = {
                        "chmod",
                        "fchmod",
};

# System calls for changing file owner
set        owner-ops = {
                        "chown", "lchown",
                        "chown32", "lchown32",
                        "fchown",
};


# System calls doing file link operations
set        link-ops = {
                        "link", "symlink",
};

# System calls for creating device files
set        mknod-ops = {
                        "mknod",
};

# System calls for opening a file
set        open-ops = {
                        "open",
};

# File renaming
set        rename-ops = {
                        "rename",
};

# File truncation
set        truncate-ops = {
                        "truncate", "truncate64",
                        "ftruncate", "ftruncate64",
};
```

```
# Unlink files
set        unlink-ops = {
                        "unlink",
};

# Deletion of directories
set        rmdir-ops = {
                        "rmdir",
};

# Mounting of filesystems
set        mount-ops = {
                        "mount",
};

# Unounting of filesystems
set        umount-ops = {
                        "umount",
                        "umount2"
};

# Changing user (-role)
set        userchange-ops = {
                        "setuid",
                        "setuid32",
                        "seteuid",
                        "seteuid32",
                        "setreuid",
                        "setreuid32",
                        "setresuid",
                        "setresuid32",
};

# Execute another program
set        execute-ops = {
                        "execve",
};

# Set real user-ID
set        realuid-ops = {
                        "setuid",
                        "setuid32",
};

# Set user-IDS in gerneral
set        setuserids-ops = {
                        "setuid",
                        "setuid32",
                        "seteuid",
                        "seteuid32",
                        "setreuid",
                        "setreuid32",
                        "setresuid",
                        "setresuid32",
```

```
};

# Set real group-ID
set        realgid-ops = {
                        "setgid",
                        "setgid32",
                        "setgroups",
                        "setgroups32",
};

# Set group-IDs in gerneral
set        setgroups-ops = {
                        "setgid",
                        "setgid32",
                        "setegid",
                        "setegid32",
                        "setregid",
                        "setregid32",
                        "setresgid",
                        "setresgid32",
                        "setgroups",
                        "setgroups32",
};

# Set other kind of privileges (capabilities)
set        privilege-ops = {
                        "capset",
};

# Change system-time
set        timechange-ops = {
                        "adjtimex",
                        "stime",
                        "settimeofday",
};


##############################################################################
##############################################################################
##############################################################################
##
## Here come the settings that trigger events
##
##

# bring sets and tags in conjunction

tag "FILE_mode"
syscall @mode-ops = always;

tag "FILE_owner"
syscall @owner-ops = always;

# tag "FILE_link"
```

```
# syscall @link-ops = always;

tag "FILE_mknod"
syscall @mknod-ops = always;

#tag "FILE_create"
#syscall open = is-o-creat(arg1);
#tag "FILE_create"
#syscall creat = always;

#tag "FILE_open"
#syscall @open-ops = always;

#tag "FILE_open"
#syscall @open-ops = (is-system-file(arg0) && !(is-rdonly(arg1)))
#                    || is-secret(arg0);

#tag "FILE_rename"
#syscall @rename-ops = always;

#tag "FILE_truncate"
#syscall @truncate-ops = always;

#tag "FILE_unlink"
#syscall @unlink-ops = always;

#tag "FS_rmdir"
#syscall @rmdir-ops = always;

tag "FS_mount"
syscall @mount-ops = always;

tag "FS_umount"
syscall @umount-ops = always;

# I think owner changing doesnt make much sense
tag "MSG_owner"
syscall msgctl = is-ipc-setperms(arg1);

tag "MSG_mode"
syscall msgctl = is-ipc-setperms(arg1);

tag "MSG_delete"
syscall msgctl = is-ipc-remove(arg1);

tag "MSG_create"
syscall msgget = always;

tag "SEM_owner"
syscall semctl = is-ipc-setperms(arg2);

tag "SEM_mode"
syscall semctl = is-ipc-setperms(arg2);
```

```
tag "SEM_delete"
syscall semctl = is-ipc-remove(arg2);

tag "SEM_create"
syscall semget = always;

tag "SHM_owner"
syscall shmctl = is-ipc-setperms(arg1);

tag "SHM_mode"
syscall shmctl = is-ipc-setperms(arg1);

tag "SHM_delete"
syscall shmctl = is-ipc-remove(arg1);

tag "SHM_create"
syscall shmget = always;

tag "PRIV_userchange"
syscall @userchange-ops = always;

tag "PROC_realuid"
syscall @realuid-ops = always;

tag "PROC_auditid"
syscall ioctl = (is-auditdevice(arg0) && is-cmd-set-auditid(arg1));

tag "PROC_loginid"
syscall ioctl = (is-auditdevice(arg0) && is-cmd-set-loginid(arg1));

tag "PROC_setuserids"
syscall @setuserids-ops = always;

tag "PROC_realgid"
syscall @realgid-ops = always;

tag "PROC_setgroups"
syscall @setgroups-ops = always;

tag "PROC_privilege"
syscall @privilege-ops = always;

tag "PROC_privilege"
syscall @priv-ops = always;

tag "SYS_timechange"
syscall @timechange-ops = always;


tag "TCP_accept"
syscall accept=always;

tag "TCP_listen"
syscall listen=always;
```

```
tag "TCP_bind"
syscall bind=always;

# not required by CAPP
# syscall ipc = always;

syscall socket = is-af-packet(arg0) || is-sock-raw(arg1);
syscall ioctl = is-sysconf-ioctl(arg1);

#
# Special filters for process/termination
event process-exit = if-crash-signal(exitcode);

#
# Events we want to log unconditionally:
event network-config = always;
event user-message = always;
event process-login = always;



predicate         is-root-uid = eq(0);
predicate         is-non-root-uid = !eq(0);
predicate        is-audit-file = prefix("/var/log/audit.d");
predicate        is-log-file = prefix("/var/log");
predicate         is-toe-file = prefix(@toe_db_files);
predicate         is-toe-dir  = prefix(@toe_db_dirs);
predicate        denied = eq(-13);
predicate         is-sysdir  = prefix(@sysdir-prefix);
predicate         cmd_trusted = prefix(@trusted_prog);

filter is-root-user  = is-root-uid(login-uid);
filter not-root-user = is-non-root-uid(login-uid);
filter effectivenonroot = is-non-root-uid(uid);
filter effectiveroot = is-root-uid(uid);


tag "AUD_file"
syscall @file-ops = is-audit-log(arg0);

tag "AUD_file"
syscall @open-ops =  is-audit-log(arg0);

tag "AUD_file"
syscall creat = is-audit-log(arg0);

tag "Open_Denied"
syscall open = denied(result) && (( not-root-user || effectivenonroot ) && is-sysdir(arg

tag "CMD_SUGID"
syscall execve = is-setuid;

# tag "CMD_priv"
```

```
# syscall execve = is-system-uid(uid);

tag "CMD_Trust"
syscall execve = cmd_trusted(arg0) && effectiveroot;

tag "TOE_file"
syscall @file-ops = is-toe-file(arg0) || is-toe-dir(arg0);

tag "TOE_file"
syscall @open-ops = ((is-toe-file(arg0) || (is-toe-dir(arg0)))  &&
                (!is-rdonly(arg1) || denied(result))) ;
tag "TOE_file"
syscall open = ((is-toe-file(arg0) || (is-toe-dir(arg0))) && is-o-creat(arg1));

tag "TOE_file"
syscall creat = is-toe-file(arg0) || is-toe-dir(arg0);
```

7.8 The file `/etc/audit/eal3files.conf`

```
# TOE config file
set toe_db_dirs = {
        "/etc/cron.d/",
        "/etc/cron.daily/",
        "/etc/cron.hourly/",
        "/etc/cron.monthly/",
        "/etc/cron.weekly/",
        "/etc/init.d/",
        "/etc/pam.d/",
        "/etc/sysconfig/",
        "/var/spool/atjobs/"
};

# TOE databases
set toe_db_files = {
        "/etc/at.deny",
        "/etc/audit/audit.conf",
        "/etc/audit/filter.conf",
        "/etc/audit/eal3files.conf",
        "/etc/crontab",
        "/etc/ftpusers",
        "/etc/group",
        "/etc/gshadow",
        "/etc/hosts",
        "/etc/inittab",
        "/etc/ld.so.conf",
        "/etc/login.defs",
        "/etc/modules.conf",
        "/etc/passwd",
        "/etc/securetty",
        "/etc/security/pam_pwcheck.conf",
        "/etc/security/pam_unix2.conf",
        "/etc/shadow",
```

```
        "/etc/ssh/sshd_config",
        "/etc/stunnel/stunnel.conf",
        "/etc/vsftpd.conf",
        "/etc/xinetd.conf",
        "/usr/lib/cracklib_dict.hwm",
        "/usr/lib/cracklib_dict.pwd",
        "/usr/lib/cracklib_dict.pwi",
        "/etc/stunnel.pem",
        "/var/log/faillog",
        "/var/log/lastlog",
        "/var/spool/cron/tabs/root",
        "/var/spool/cron/allow",
        "/var/spool/cron/deny"
};


# Trusted programs
set  trusted_prog = {
        "/bin/date",
        "/bin/login",
        "/bin/ping",
        "/bin/su",
        "/sbin/agetty",
        "/sbin/auditd",
        "/sbin/init",
        "/sbin/mingetty",
        "/usr/bin/amtu",
        "/usr/bin/at",
        "/usr/bin/chage",
        "/usr/bin/chfn",
        "/usr/bin/chsh",
        "/usr/bin/crontab",
        "/usr/bin/gpasswd",
        "/usr/bin/passwd",
        "/usr/sbin/stunnel",
        "/usr/sbin/atd",
        "/usr/sbin/audbin",
        "/usr/sbin/aucat",
        "/usr/sbin/augrep",
        "/usr/sbin/aurun",
        "/usr/sbin/cron",
        "/usr/sbin/groupadd",
        "/usr/sbin/groupdel",
        "/usr/sbin/groupmod",
        "/usr/sbin/sshd",
        "/usr/sbin/useradd",
        "/usr/sbin/userdel",
        "/usr/sbin/usermod",
        "/usr/sbin/vsftpd",
        "/usr/sbin/xinetd"
};

# system directories
set sysdir-prefix = {
```

```
        "/bin",
        "/boot",
        "/dev",
        "/etc",
        "/lib",
        "/opt",
        "/proc",
        "/root",
        "/sbin",
        "/usr",
        "/var/adm",
        "/var/log"
};
```