

SLES Security Guide

Klaus Weidner <klaus@atsec.com>

August 1, 2003

atsec is a trademark of atsec GmbH

IBM, BladeCenter, and xSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., in the United States, other countries, or both.

Linux is a registered trademark of Linux Torvalds.

UNIX is a registered trademark of The Open Group in the United States and other countries.

This document is provided "AS IS" with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Copyright (c) 2003 by atsec GmbH, and IBM Corporation or its wholly owned subsidiaries.

Contents

1	Introduction	5
1.1	Purpose of this document	5
1.2	How to use this document	5
1.3	What is a CC compliant System?	5
1.4	Requirements for the system's environment	6
1.5	Requirements for the system's users	6
2	Installation	7
2.1	Supported hardware	7
2.2	Selection of install options and packages	7
2.3	Installing required updates.	9
2.4	Getting the necessary updates	10
2.5	Verifying and installing the updates	11
3	Secure initial system configuration	11
3.1	Automated configuration of the system	11
3.2	Remove packages	12
3.3	Disable services	14
3.4	Remove setuid/setgid root settings from binaries	14
3.5	Update permissions for 'su'	15
3.6	Disable root login over the network	15
3.7	Setting up SSH	16
3.8	Setting up xinetd	17
3.9	Setting up FTP	17
3.10	Setting up Postfix	18
3.11	Introduction to Pluggable Authentication Module (PAM) configuration	18
3.12	Required Pluggable Authentication Module (PAM) configuration	19
3.13	Setting up login controls	23
3.14	Configuring the GRUB boot loader	24
3.15	Reboot and initial network connection	25
4	System operation	25
4.1	System startup, shutdown and crash recovery	25
4.2	Backup and restore	25
4.3	Gaining superuser access	26
4.4	Installation of additional software	26
4.5	Scheduling processes using <code>cron</code> and <code>at</code>	27
4.6	Mounting filesystems	28
4.7	Managing user accounts	29
4.8	SYSV shared memory and IPC objects	30
5	Monitoring, Logging & Audit	30
5.1	Reviewing the system configuration	30
5.2	System logging and accounting	31
5.3	System configuration variables in <code>/etc/sysconfig</code>	32
6	Security guidelines for users	35
6.1	Online Documentation	35
6.2	Authentication	36
6.3	Password policy	36
6.4	Access control for files and directories	37
6.5	Data import / export	38

7	Appendix	38
7.1	Online Documentation	38
7.2	Literature	39
7.3	The script <code>/usr/lib/eal2/bin/sles-eal2</code>	39
7.4	The file <code>/etc/permissions.eal2</code>	39

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.

- The hardware **MUST** be the one of the following IBM® xSeries™ systems:

```
Universal x205, x225, x235, x255, x305
Rack-optimized x335, x345, x360
Scalable x440 Entry, x440
BladeCenter(TM) HS20
```

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.

- 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).
- 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.
- 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.

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 "Security guidelines for users" (§6) 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.

2 Installation

The evaluation covers a fresh installation of the SLES version 8 on an IBM xSeries System using Intel™Pentium™4 or XEON processors. This **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, IEEE1394/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.

SLES 8 is shipped on four CDs. The first CD is the SuSE SLES addition to the UnitedLinux Distribution distributed on the other three CDs. Note that the UnitedLinux CDs numbered 1 to 3 are labeled as SuSE CDs 2 to 4 in the CD set.

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 x86". It is shipped in a sealed sleeve.
- Insert the SLES 8 CD, boot from CD-ROM. Text mode **MAY** be chosen instead of the default graphical 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", and confirm the choice.
- 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
sles-admin-x86+x86-64_en # RECOMMENDED: Online Administrator Manual
sles-inst-x86+x86-64_en  # RECOMMENDED: Online Installation Manual
man-pages               # RECOMMENDED: Manual pages
howtoenh                # RECOMMENDED: Online how-to documentation
lprng                   # OPTIONAL: Print spooler
xinetd                  # OPTIONAL: Inetd (only used for vsftpd)
vsftpd                  # OPTIONAL: FTP daemon (needs xinetd)

```

Bootimg: 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 "Setting up login controls" (§3.13): . Close the dialog.
 - press the "Next" button to continue.
- Network cards configuration
 - Configure all installed network cards (zero or more)
 - 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.
 - The network connections MUST remain disconnected until the post-install system configuration is finished. Exception: You MAY set up a temporary connection to a server for download of required patches if that server is in an evaluated configuration and not accessible for non-administrative users over the network or serial terminals.

2.3 Installing required updates.

The base system from CD is not yet configured to meet the requirements for the installation. By installing the *certification-sles-eal2* RPM and the prerequisite dependencies (which are security fixes on top of SLES 8) the system is brought up to the level needed for running it in the evaluated configuration.

2.4 Getting the necessary updates

The following security updates **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 **RECOMMENDED** method is to use the *certification-sles-eal2* RPM package which contains the *sles-eal2* script and the required update RPMs in a single package. If that package is not available, you **MAY** also perform the upgrade manually as described below.

The individual updated packages are available from the SuSE maintenance web (requires authentication):

<http://sdb.suse.de/download/i386/update/SuSE-SLES/8/rpm/i586/>

Choose **ONE** of the following kernel packages depending on your hardware:

<code>k_deflt-2.4.19-288.i586.rpm</code>	<code># uniprocessor</code>
<code>k_smp-2.4.19-288.i586.rpm</code>	<code># SMP (multiprocessor)</code>

Choose **ONE** of the following glibc upgrades:

<code>glibc-2.2.5-179.i686.rpm</code>	<code># Pentium Pro, II, III, 4 or Xeon CPU</code>
<code>glibc-2.2.5-179.i586.rpm</code>	<code># other Pentium-compatible CPU</code>

In addition, download the following updated packages:

```
aaa_base-2003.3.27-2.i586.rpm
bc-1.06-498.i586.rpm
file-3.37-206.i586.rpm
freetype2-2.0.9-87.i586.rpm
grub-0.92-169.i586.rpm
hwinfo-5.43-5.i586.rpm
iproute2-2.4.7-495.i586.rpm
kbd-1.06-169.i586.rpm
libgcc-3.2.2-5.i586.rpm
libstdc++-3.2.2-5.i586.rpm
net-tools-1.60-348.i586.rpm
openldap2-client-2.1.4-70.i586.rpm
openssl-0.9.6g-69.i586.rpm
pam-modules-2002.8.28-0.i586.rpm
perl-5.8.0-115.i586.rpm
readline-4.3-53.i586.rpm
shadow-4.0.2-300.i586.rpm
star-1.4.2-2.i586.rpm
sysconfig-0.23.22-17.i586.rpm
timezone-2.2.5-179.i586.rpm
w3m-0.3.1-105.i586.rpm
wget-1.8.2-146.i586.rpm
yast2-bootloader-2.6.65-7.i586.rpm
yast2-core-2.6.56-3.i586.rpm
yast2-country-2.6.35-1.i586.rpm
```

```
yast2-installation-2.6.94-2.i586.rpm
yast2-ncurses-2.6.24-19.i586.rpm
yast2-online-update-2.6.15-25.i586.rpm
yast2-packagemanager-2.6.49-0.i586.rpm
yast2-storage-2.6.56-0.i586.rpm
yast2-update-2.6.23-2.i586.rpm
yast2-users-2.6.33-18.noarch.rpm
```

The versions used **MUST** exactly match those listed here for the evaluated configuration.

After you have downloaded the packages from the Internet, transfer them to the target server, i.e. by using a CD-R.

2.5 Verifying and installing the updates

Before installing the patches and the *certification-sles-eal2.rpm*, the integrity of the packages **MUST** be checked. If you have done an online update from an internal mirror, the online update tool will have verified the signatures automatically, but you **MAY** also verify the files in */var/lib/YaST2/you/i386/update/SuSE-SLES/8/rpm/i586/* manually.

Use the *rpm(8)* command with the `--checksig` flag to verify the downloaded RPM files:

```
rpm --checksig *.rpm || echo 'Check failed!'
```

This will verify that the packages were signed with the SuSE build key and will detect if they have been tampered with. If the message `Check failed!` is printed, you **MUST NOT** proceed with the update.

If the verification step reported that all packages are signed correctly, proceed with the upgrade:

```
rpm -U *.rpm
```

The new kernel will be activated after rebooting, which is **REQUIRED** after the initial system configuration in the next chapter is completed.

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-eal2.rpm* package **MUST** be installed initially to achieve the evaluated configuration. This RPM package contains updates to the manuals, EAL2 specific configuration files and scripts to set up the evaluated configuration.

Please check the file */usr/share/doc/packages/certification-sles-eal2/README-eal2.txt* from the *certification-sles-eal2.rpm* for the latest errata information.

The *certification-sles-eal2.rpm* package will contain a setup script that has to be run to implement the evaluated configuration: */usr/lib/eal2/bin/sles-eal2*.

The *certification-sles-eal2* RPM contains the following EAL2 specific configuration files:

/etc/permissions.eal2

We RECOMMEND that you use the `sles-eal2` script to reset the configuration to its initial state after any updates, but you MAY also perform the steps listed here manually. If you use the script, the remaining steps in this chapter are done automatically; skip ahead to the "System operation" chapter (§4).

3.2 Remove packages

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.

The evaluated configuration consists of exactly the following packages:

UnitedLinux-build-key	netcfg
aaa_base	openldap2-client
aaa_skel	openssh
acl	openssl
ash	pam
at	pam-modules
attr	parted
bash	pciutils
bc	pcre
bzip2	perl
certification-sles-eal2	permissions
cpio	popt
cracklib	postfix
cron	ps
curl	readline
cyrus-sasl	rpm
db	sed
devs	sh-utils
dialog	shadow
diffutils	sitar
e2fsprogs	sles-admin-x86+x86-64_en
ed	sles-inst-x86+x86-64_en
file	sles-release
filesystem	star
fileutils	suse-build-key
fillup	sysconfig
findutils	syslogd
freetype2	sysvinit
gawk	tar
gdbm	telnet
glibc	terminfo
gpg	texinfo
gpm	textutils
grep	timezone
groff	unitedlinux-release
grub	utempter
gzip	util-linux
hdparm	vim
heimdal-lib	vsftpd

howtoenh	w3m
hwinfo	wget
iproute2	xinetd
iputils	yast2
isapnp	yast2-bootloader
k_deflt	yast2-core
k_smp	yast2-country
kbd	yast2-installation
ksymoops	yast2-mouse
l2h-pngicons	yast2-ncurses
less	yast2-network
libgcc	yast2-online-update
libstdc++	yast2-packagemanager
libxcrypt	yast2-packager
libxml2	yast2-pam
liby2util	yast2-runlevel
logrotate	yast2-security
lprng	yast2-storage
lukemftp	yast2-sysconfig
m4	yast2-theme-SuSELinux
mailx	yast2-theme-UnitedLinux
man	yast2-trans-en_US
man-pages	yast2-transfer
mktemp	yast2-update
modutils	yast2-users
ncurses	yast2-xml
net-tools	zlib
netcat	

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 "Installation of additional software" (§4.4) 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-ea12` script does not remove these packages if they are installed on the system:

```

binutils
cpp
expect
flex
gcc
gcc-c++
glibc-devel
libstdc++-devel
make
tcl
tk
xshared

```

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 servers are allowed for runlevel 3:

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

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

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/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
/usr/sbin/postqueue
```

For informational purposes, here is a non authoritative 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
/usr/sbin/utempter

```

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

```

Then run `chkstat -set /etc/permissions.eal2` to set the needed SUID and SGID bits.

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

```

CHECK_PERMISSIONS=set
PERMISSION_SECURITY="eal2"

```

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 "Gaining superuser access" (§4.3) 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/securettys` 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.

Authentication mechanisms other than User/Password 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
PermitRootLogin no
RSAAuthentication no
PubkeyAuthentication no
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 is not checked by the ftp daemon itself but by a PAM module. Please see the section "Required PAM configuration" (§3.12) 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 EAL2 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 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.

3.12 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 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 the pam configuration files:

/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_unix2.so
```

```
password required    pam_pwcheck.so
password required    pam_permit.so
session  required    pam_deny.so
```

/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_pwcheck.so
password  required      pam_unix2.so    use_first_pass use_authtok
session   required      pam_deny.so
```

/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_pwcheck.so
password  required      pam_unix2.so    use_first_pass use_authtok
session   required      pam_deny.so
```

/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  required      pam_pwcheck.so
password  required      pam_unix2.so    use_first_pass use_authtok
session   required      pam_unix2.so
session   required      pam_limits.so     # optional
```

/etc/pam.d/other

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

/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  required      pam_pwcheck.so
password  required      pam_unix2.so      use_first_pass use_authtok
session   required      pam_unix2.so
```

/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
password  required      pam_pwcheck.so
password  required      pam_unix2.so      use_first_pass use_authtok
session   required      pam_unix2.so
session   required      pam_limits.so      # optional
```

/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_unix2.so
session   required        pam_unix2.so

```

Forcing the root user to change the root password is not desired here, therefore the *pam.pwcheck.so* module is absent.

/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

```

Forcing the root user to change the root password is not desired here, therefore the *pam.pwcheck.so* module is absent.

/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
password  required        pam_unix2.so
session   required        pam_unix2.so

```

Note that the FTP protocol has no provisions for changing passwords, therefore the *pam.pwcheck.so* module is absent.

/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

```

/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
```

3.13 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 EAL2 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 displly unknown user names on failed log ins
LASTLOG_ENAB	yes	Log last log in
OBSOURE_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

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 wordlists. Suggested wordlists 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.

3.14 Configuring the GRUB 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 hard disk containing SLES, and not from floppy disks or CD-ROMs. Ensure that this setting cannot be modified, i.e. by using a BootProm/BIOS password to protect access to the configuration.
- 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
```

Example configuration:

```
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$O4711/$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 Reboot and initial network connection

After all the changes described in this chapter have been done, reboot the system to ensure that all unwanted tasks are stopped. The system will then match the evaluated configuration. The server MAY now 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

When powered on, the system will boot into the SLES operating system automatically. 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 (booting from floppy disk or CD-ROM, i.e. to replace a defective hard drive), the appropriate selections can be made from the *grub(8)* menu at boot.

If the system is not able to boot due to a corrupted configuration (due to a mistake in administration, or a crash), you can use the *grub(8)* bootloader on the console to circumvent the normal boot process, and manually restore a working configuration. The following grub command line launches a shell directly from the kernel and bypasses the normal init/login mechanism:

```
grub> kernel /boot/vmlinuz root=/dev/hda1 init=/bin/sh
```

Please refer to the section "Configuring the GRUB boot loader" (§3.14) for more information.

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

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 "Data import / export" (§6.5). Regular backups of the following files and directories (on removeable media such as CD-R, or on a separate host) are RECOMMENDED:

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

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 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.

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 *fiok*(3) manual pages.

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/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/spool/atjobs/*
/var/spool/cron/*
/var/spool/cron/allow
/var/spool/cron/deny

```

Use the commands `faillog` and `lastlog` to detect unusual patterns of login attempts or an unexpectedly large number of login failures.

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
boot.msg	Messages from system startup
faillog	Failed log ins of known users, (see <code>faillog(8)</code>)
lastlog	Last successful log in (see <code>lastlog(8)</code>)
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 subsystem, see <code>who(1)</code>
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 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.

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:

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

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="eal2"
```

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:

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

language

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

backup

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

boot

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

displaymanager

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

kernel

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

clock

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

proxy

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

windowmanager

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

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.

java

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

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.
```

hardware

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

printer

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

news

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

console

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

keyboard

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

mouse

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

lvm

Sets up LVM. Not used in the evaluated configuration.

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).

syslog

Configures the *syslog* daemon. **MAY** be changed.

SuSEfirewall2

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

hotplug

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

ssh

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

postfix

Configures the basic MTA setup. MUST NOT be changed.

bootloader

Configures the type of bootloader to use and where to store the boot record. 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.

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

You **MAY** also 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.

- Your password **MUST** be a minimum of 8 characters in length. More than 8 characters **MAY** be used, 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 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-eal2/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® 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/eal2/bin/sles-eal2`

7.4 The file `/etc/permissions.eal2`