

# IPWorks OS Hardening Guide for KVM

---

## USER GUIDE

**Copyright**

© Ericsson AB 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

**Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Prerequisite	1
1.2	Related Information	1
<b>2</b>	<b>System Configuration Process Overview</b>	<b>3</b>
<b>3</b>	<b>Installation</b>	<b>5</b>
3.1	Installing Required System and Software Components	5
3.2	Installing Additional Security-Enhancing Packages	5
3.3	Installing SUSE Patches	6
<b>4</b>	<b>System Configuration</b>	<b>9</b>
4.1	Disabling Standard Boot Time Services	9
4.2	TCP Wrappers	10
4.3	Checking System Sockets	10
4.4	Logging	10
4.5	File Systems	12
4.6	System Access, Authentication and Authorization	14
<b>5</b>	<b>SLES Firewall (Optional)</b>	<b>17</b>
<b>6</b>	<b>SSH Configuration</b>	<b>19</b>
6.1	Configuring SSH for SSH2-only Access	19
6.2	Limiting SSH Access	19
<b>7</b>	<b>Security Enhancement and Auditing Tools</b>	<b>23</b>
7.1	Seccheck	23
7.2	AIDE	23
7.3	Audit Event	24
7.4	Password Checking Tools	24
<b>8</b>	<b>Physical Security (Optional)</b>	<b>25</b>
8.1	Editing BIOS to Disallow Booting from CDROM/Floppy/USB/Network	25
8.2	Setting GRUB Password	25
<b>9</b>	<b>Post Hardening Activities</b>	<b>27</b>



9.1	Rebooting System	27
9.2	Deploy IPWorks VNF	27
	<b>Reference List</b>	<b>29</b>



# 1 Introduction

This document provides step-by-step instructions to harden the SLES 12 SP2 platform used for the IPWorks application. This means configuring the node to a generally agreeable security level.

The issues dealt with here are applicable to security patches, configuring the operating system services, managing user accounts and permissions, and installing additional third party security software.

The fundamental principle to be followed is “the more minimal, the more secure”.

For Additional node and application specific hardening information, refer to *IPWorks Application Components Hardening Guide*, Reference [4].

## 1.1 Prerequisite

The personnel following these instructions must be familiar with:

- Working in UNIX-like environment without X-Windowing system.
- Using yast in character mode.
- UNIX shell commands.

**Note:** It is recommended to create the backup file whenever to modify a configuration file.

## 1.2 Related Information

Trademark information, typographic conventions, and definition and explanation of abbreviations and terminology can be found in the following documents:

- *Trademark Information*, Reference [1]
- *Typographic Conventions*, Reference [2]
- *Glossary of Terms and Acronyms*, Reference [3]





## 2 System Configuration Process Overview

Figure 1 describes the configuration process of Node Hardening:

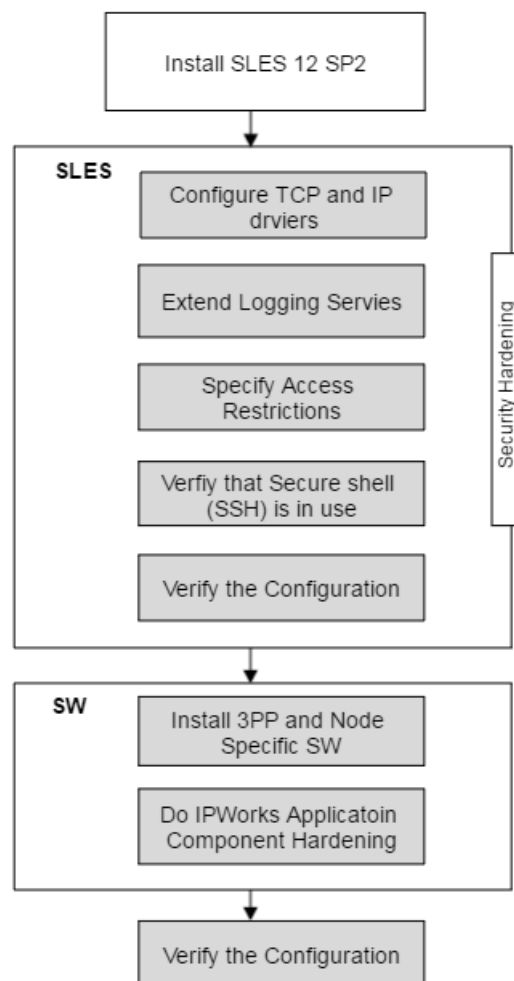


Figure 1 Configuration Process of Node Hardening





## 3 Installation

### 3.1 Installing Required System and Software Components

The system security begins with installation.

The installation only concerns required system and software components and can be supplemented afterwards if application software requires additional packages. For more information about installation procedure, refer to section *Installing SUSE Linux Enterprise Server 12 SP2 for x86 (64-bit)*, IPWorks OS Installation Instruction for KVM, Reference [5].

### 3.2 Installing Additional Security-Enhancing Packages

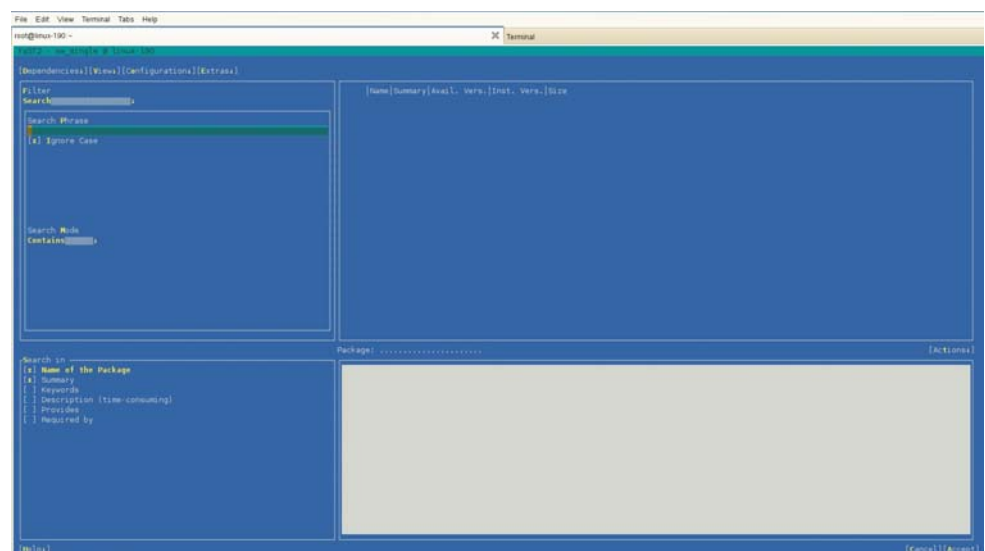
Steps are listed as follows:

1. Put installation DVD in and start YaST.

```
# yast sw_single
```

Click **Search** and search for **AIDE**.

Select **aide** and click on **Accept**. Proceed with **Continue**.



2. Follow the same procedure for:
  - clamav (Antivirus toolkit).

- seccheck (SUSE customized scripts that perform various security checks).
3. Verify the following packets are already installed with the base package:

- cracklib (Utilities to prevent users from choosing easily guessed passwords).

```
# rpm -qa |grep cracklib

cracklib-dict-full-2.8.12-63.17.x86_64

cracklib-2.9.0-7.1.x86_64
```

- SuSEfirewall (SuSE's front end for iptables/ip6tables firewall).

```
# rpm -qa |grep SuSEfirewall

SuSEfirewall2-3.6.312-1.3.noarch
```

- rsyslog (advanced system logger).

```
# rpm -q rsyslog

rsyslog-8.4.0-14.1.x86_64
```

### 3.3 Installing SUSE Patches

1. Download the OS patches ("IPWorks 2 SLES 12 SP2 Update Patch") from the SW Gateway.

IPWorks software packages can be retrieved from SW Gateway. For specific information, see the product release notes.

2. Transfer the package of the OS patches to a target host.

```
# scp 19010-CXP9034019_3_Ux_<Revision Number>.tar.gz
<username>@<Host_addr>:/<path>
```

For example:

```
# scp 19010-CXP9034019_3_Ux_B.tar.gz root@<Host_addr>:/
tmp
```

3. Unpack the package.

```
# ssh root@<Host_addr>

# cd /tmp

# tar -zxvf /tmp/19010-CXP9034019_3_Ux_B.tar.gz
```



4. Use md5sum command to check each patch file, the expected results are in `checksum_result.txt`.
5. Install the OS patches.  
  
# `cd /tmp/rpms`  
  
# `./rpms_upgrade.sh`





## 4 System Configuration

### 4.1 Disabling Standard Boot Time Services

A service program, generally called daemon, is initialized when the machine is booted up. Some daemons must be closed when the system is hardened to the production network. SLES 12 as well as other Unix-like machines has different initial boot levels where the daemons are activated.

From security point of view the unused daemons must be closed because they increase potential compromised risk in the system:

1. Open YaST.

```
# yast
```

Select **System> Services Manager**

```
auditd
irqbalancer
nfs
nscd
smartd
xinetd
```

**Note:** The services must be re-enabled if it is required by the IPWorks application software. Read the information field carefully for which usage the service is needed.

2. Select and disable the following services:
3. Select **Expert mode** and set default runlevel after booting to 3: Full multiuser with network.

**Note:** Several other services can be started manually to help the testing process. After the installation or testing, these services might be left running. All the manually-started unnecessary services (from system point of view) must be eventually deactivated after installation/testing to minimize possible attack vectors.

Also, it is somewhat acceptable (and sometimes even necessary) that in test lab environment all the security policies are not followed that strictly as in production environment. For example, Firewalls and a bit easier typed passwords.



## 4.2 TCP Wrappers

TCP Wrappers can be used to control many services including SSH access, and particular IP addresses or networks.

See [man tcpd](#) for information on how to configure the files `/etc/hosts.allow` and `/etc/hosts.deny` to enforce this.

Define TCP wrapper to restrict non-authorized incoming connection attempts to the system.

Steps are listed as follows:

- Edit the file `hosts.allow` into the directory `/etc/` and add host names or IP addresses with the netmasks of the machines.

```
ALL: <trusted_ip_address1, trusted_ip_address2>
```

- Edit the file `hosts.deny` in the directory `/etc/` and add a line that denies incoming connection attempts:

```
ALL: ALL
```

- Verify the file permission and the owner rights.

See Section 6 on page 19.

## 4.3 Checking System Sockets

The most important check is being performed when checking the active services/ports on the system. The unnecessary services/ports must be closed. Verify the system sockets (interfaces) with the following command:

```
# netstat -nap | grep LISTEN
```

There must be only specific ports in a listen mode , for example, the above command can return only the accepted port information.

Make sure there is no unintended services enabled, for example, the default configuration does not use all possible insecure services. Go through Section 4.1 on page 9 to automatically start services at boot time once again if there are some unrecognized open ports/services.

## 4.4 Logging

System logging records different and specific activities from the system. It is often necessary to correlate log information to many different systems (particularly after a security incident).



#### 4.4.1 Rsyslog Configuration

Rsyslog offers many different kind of logging features for use. Some of these logging services are crucial, especially after a security incident.

The rsyslog configuration includes a facility of the operating system event that needs to be defined for the system security. Following facilities are used:

Facility	Message Category
Auth or security	Authorization/security
Authpriv	Authorization/privacy security
Cron	Cron daemon messages
Daemon	System daemon-generated messages
Kern	Kernel messages
Syslogd	Syslogd generated messages
User	User program generated messages

The rsyslog configuration includes a message priority of the facility that needs to be defined for the system security. Following priorities are used:

Priority	Message Type
Emerg	System is unstable
Alert	Immediate attention required
Crit	Critical conditions
Err	Error status messages
Warning	Warning messages
Notice	Normal but important conditions
Info	Informational status messages

Usage of `rsyslog` is recommended and hence for configuration the documentation is included within the package.

Verify the installation of rsyslog:

```
# rpm -q rsyslog
```

#### 4.4.2 Logging Information

The logging system shall be used to explore system events, especially the unauthorized attempts and file modifications. The log file configuration in the `/etc/rsyslog/rsyslog.conf` is important to protect the operating system.

It is critical to protect system log files from being modified by unauthorized users. Also certain logs contain sensitive data that should only be available to the system administration personnel. From the entire system point of view it is important to check all log file permissions.

Generous log file permissions can weaken the ability to detect suspicious behavior in the operating system. Avoid `world` read and write permissions.

Verify that all log files have proper file permissions by:

- Changing the privileges for all the log files if necessary:

```
# chmod 600 <log_file>
```

## 4.5 File Systems

### 4.5.1 File Permissions

Permissions on system files need to be set correctly so that a user or process cannot make unauthorized changes to these files. Most of the permissions setting are automatically properly set during operating system installation. However, SUSE systems have various levels of pre-set permissions, which are defined in the files `/etc/permissions`, `/etc/permissions.easy`, `/etc/permissions.local`, `/etc/permissions.secure` and `/etc/permissions.paranoid`.

There are also some permission settings defined for the operation of particular programs in files under `/etc/permissions.d/`.

Set permissions to secure settings by executing the following command:

```
# chkstat -set /etc/permissions.secure
```

Permissions can also be set as:

- `yast: Security and Users >`

**OR**

- `yast: System > /etc/sysconfig Editor`

There are a small number of files that need to have SUID root permissions set: such programs are a possible attack vector: you can check which files on the system have SUID permissions with a command such as:

```
# find / -type f -perm -u=s -ls
```

Files that are both executable and writable by others can be found using

```
# find / -type f -perm -o=w,u=x -ls
```



It's critical to protect system log files from being modified by unauthorized individuals. Also, certain logs contain sensitive data that should only be available to the system administrator. From the entire system point of view it is important to check the file permissions.

## 4.5.2 System Information

Operating system will be more secure when no system information is revealed to anyone on the network.

The file `/etc/motd` shall not have any details that reveal the software version run on the host. It is recommended to keep the file empty.

Verify that the release files have file permissions set for the owner only:

```
# ls -al /etc/*release
# chmod 400 /etc/*release
```

Verify the Banner option is commented with the hash sign in the file `/etc/ssh/sshd_config` like

```
# Banner none
```

Edit `/etc/issue` file so that it does not reveal any valid information about the system, hardware or software versions. Keep the file empty or optionally populate it with nonsense information.

## 4.5.3 Secure Shell files

The following files are important for the entire system and therefore their file permissions and file ownership must be checked.

<code>/etc/ssh/sshd_config</code>	<code>-rw-r----</code>	root
<code>/etc/ssh/ssh_host_key</code>	<code>-rw-----</code>	root
<code>/etc/ssh/ssh_host_dsa_key</code>	<code>-rw-----</code>	root
<code>/etc/ssh/ssh_host_rsa_key</code>	<code>-rw-----</code>	root
<code>/etc/ssh/ssh_host_key.pub</code>	<code>-rw-r--r--</code>	root



## 4.6 System Access, Authentication and Authorization

### 4.6.1 User Account Status

Accounts that are not used must be removed. Only few accounts should have a password string, for example, root and ipworks user. The user must have a strong encrypted password.

List every account in a file `/etc/passwd`, `/etc/shadow` and `/etc/group`.

For example

```
# less /etc/passwd
```

```
# less /etc/shadow
```

```
# less /etc/group
```

### 4.6.2 Remove Unnecessary Accounts

The user accounts are checked and verified that no plain password exist.

Remove, lock, or comment out unnecessary accounts, including "bin", "games", "news", "daemon", "lp", "mail", "postfix", "uucp" and "wwwrun". Also set the login shell for all of the accounts above to `/bin/false` in `/etc/passwd`. Removal of user accounts and passwords minimizes the risk of compromised account(s) in the system with the command `userdel`.

```
# userdel <account name>
```

List the contents of file `/etc/passwd`, `/etc/shadow` and `/etc/group` and verify no unnecessary accounts are standing on the list.

### 4.6.3 Restrict Shell Alternatives for Accounts

The file `/etc/shells` keeps information about valid shells. Different system services and accounts use shells.

Verify that a proper shell exists for every account in the file `/etc/shells`. Verify that accounts which are not supposed to have login shell have `/bin/false` as default shell. The shell for every account is defined in the file `/etc/passwd`.

### 4.6.4 Required Strongest Possible Passwords

The default password length must meet all the following conditions:

- At least 10 characters



- Upper case characters
- Lower case characters
- Numbers
- Special Characters

yast: **Security and Users > Security Center and Hardening > Password settings.**

Verify the followings parameters:

- Check new passwords
- Test for complicated passwords
- Number of passwords to remember: 10
- Password encryption method Blowfish
- Minimum acceptable password length: 10

#### 4.6.5 Timeout in Bash shell

You must enable automatic logout after specific inactivity time for the bash shell from `/etc/profile`.

1. Create the file `profile.local` to the `/etc/`.

```
# touch /etc/profile.local
```

2. Use the `echo` command to add the following lines.

```
# echo 'TMOUT=600' > /etc/profile.local
```

```
# echo 'export TMOUT' >> /etc/profile.local
```

```
# chmod +x /etc/profile.local
```

**Note:** This does not affect other shells and can be overridden in the users' `.profile` file.

3. Login again to make the configuration take effect.

#### 4.6.6 Protection against Brute Force Attacks

yast > **Security and Users > Security Center and Hardening > Login Settings.**

Do the followings:

1. Set Delay after Incorrect Login Attempt to 3.



2. Disable Allow Remote Graphical login.
3. Set and verify the login timeout `/etc/login.defs`:

```
LOGIN_TIMEOUT 60 (default)
```

#### 4.6.7

##### Telnet

This services should not be used. Use sftp, scp and ssh instead. TELNETD server is not enabled by default in SUSE.

- For TELNETD, check whether it is in use:

```
# /etc/init.d/xinetd status
```

The expected result:

No such file or directory

Otherwise, stop it:

```
# /etc/init.d/xinetd stop
```



## 5 SLES Firewall (Optional)

A server which is available from the internet can be protected by the firewall. On a SLES system you can create a firewall simply using the SuSEfirewall2 package which creates iptables (netfilter) and ip6tables rules based on your own specifications. You can also if you wish create your own script to set up the iptables/ip6tables rules without using SuSEfirewall2.

Any firewall rules you set up must be thoroughly tested. Documentation on SuSEfirewall2 is included in the SLES 12 manual. Extensive documentation on the use of iptables/ip6tables is available at <http://www.netfilter.org/documentation/index.html>.

To verify that the file `/etc/sysconfig/SuSEfirewall2` has following definition:

```
FW_SERVICES_REJECT_EXT=""
```

This can also be done in `yast's /etc/sysconfig` editor.

Configure the other firewall settings in yast: **Security and Users > Firewall**.





## 6 SSH Configuration

### 6.1 Configuring SSH for SSH2-only Access

Modify the file `/etc/ssh/sshd_config` to change the `PROTOCOL` line from:  
**#Protocol 2** to: **Protocol 2**

### 6.2 Limiting SSH Access

#### 6.2.1 Change SSH Port

If it is necessary to change the default SSH port, this change is done in the file `/etc/ssh/sshd_config`. First uncomment the line and then change port 22 to a specific port, store the file and restart SSH daemon 2.

```
rcsshd restart
```

#### 6.2.2 Limit by Users

To limit SSH access by adding users (non-root) to a specific group, apply one of the following approaches:

*In yast tool:*

1. Select **Security and Users > User and Group Management > Groups**.
2. Add a group named "sshlogin", then type and confirm the password.
3. Select **Security and Users > User and Group Management > Users**.
4. Add a user named "support", then type and confirm the password.
5. **Edit** the "support" user, locate to the **Details** tab, and then select the groups "sshlogin" and "ipworks" from the **Additional Groups** pane.
6. Copy the file `/root/.bashrc` to `/home/support/` for replacing the original file `.bashrc` by the command:

```
# cp /root/.bashrc /home/support/.bashrc
```

*In Command Line:*

1. Add a group named "sshlogin":

```
# groupadd sshlogin
```

*TIP:* Use the command `grep sshlogin /etc/group` to check whether the group is added successfully.

2. Add a user named "support":

```
# useradd -m support
```

3. Set password for the user "support".

```
# passwd support
```

4. Add the user "support" to the groups "sshlogin" and "ipworks":

```
# usermod -G sshlogin support
```

*TIP:* Use the command `grep sshlogin /etc/group` to check whether the user is added to the group successfully.

### 6.2.3 Sshd\_config Modification

Some SSH modification must be done in the file `/etc/ssh/sshd_config`, see Reference [8]. `PermitRootLogin` option is set to "no", the root is not allowed to log in.

Change the line from:

```
# PermitRootLogin yes
```

**To:**

```
PermitRootLogin no
```

Specified login is allowed only for users whose primary group or supplementary group list matches.

Create a following line:

```
AllowGroups sshlogin
```

**Note:**

- Root user cannot login SSH if this line is added to the file `/etc/ssh/sshd_config`.
- Since some operation needs to use root SSH authority, it is recommended to do the configuration after IPWorks installation and initial configuration.

Finally as root restart sshd:

```
# rcsshd restart
```



## 6.2.4 Limit by Hosts

In `/etc/hosts.allow`, enter the following lines for the hosts you specifically allow.

For example:

```
sshd : 127.0.0.1 : allow
sshd : 192.168. : allow
sshd : 130.57.5.70 : allow
sshd : 10. : allow
```

Next enter that all other need to be denied:

```
sshd : ALL :deny
```

Pay attention to the following work precedence:

- The system allows the SSH login attempt if the host applies to `/etc/hosts.allow`.
- The system denies the SSH login attempt if the host does not apply to `/etc/hosts.allow` and apply to the `/etc/hosts.deny`.
- The system allows the SSH login attempt if the host does not apply to both `/etc/hosts.allow` and `/etc/hosts.deny`.

## 6.2.5 SSH Systematic or Brute-Force Attack Protection (Optional)

It is possible to apply firewall rules that detect and prevent more than a defined number of connection attempts from a particular host in a particular time period:

In this example the default SSH port is used in the IPWorks application. If the default SSH port has been changed to another port number (see `/etc/ssh/sshd_config`), that must be taken into consideration in the `dport` parameter value. Also the following firewall rules need to be placed in the correct row of the iptables INPUT chain.

```
iptables -N external
iptables -A external -i eth0 -p tcp --dport 22 -m state --state NEW
iptables -A external -i eth0 -p tcp --dport 22 -m state --state NEW
iptables -A external -i eth0 -p tcp --dport 22 -m state --state NEW
```

These rules prevent more than 4 connection attempts per 10 minute period from a particular IP number.

If possible, it is advisable to switch off username / password authentication for SSH with the line: `ChallengeResponseAuthentication no` Then only public/private key-pair authentication will be possible, and brute force attacks cannot take place.

More information on protecting SSH against brute-force attacks, refer to this article: [http://en.opensuse.org/SDB:SSH\\_systematic\\_attack\\_protection](http://en.opensuse.org/SDB:SSH_systematic_attack_protection)



## 6.2.6 SSH Server Strict Modes

Ensure secure permissions on a user's `.ssh` directory.

In `/etc/ssh/sshd_config`, modify:

```
# StrictModes yes
```

**To:**

```
StrictModes yes
```

Then restart ssh server:

```
# rcsshd restart
```



## 7 Security Enhancement and Auditing Tools

### 7.1 Seccheck

Varieties of system security checks are included in the functionality of the seccheck package.

Verify installation of seccheck:

```
# rpm -q seccheck
```

If not installed, see Section 3 on page 5.

In file `/etc/sysconfig/seccheck`, change the parameter `START_SECCHK` from **yes** to **no**.

This prevents seccheck to run automatically as a cronjob, but the administrator can run it manually.

Run seccheck regularly as root user:

```
/usr/lib/secchk/security-daily.sh
```

```
/usr/lib/secchk/security-weekly.sh
```

```
/usr/lib/secchk/security-monthly.sh
```

**Note:** When running the seccheck, if the system receives the error "Password security checking not possible, package john not installed", perform the following:

- a Open the link: [http://download.opensuse.org/repositories/security/SLE\\_12\\_SP2/x86\\_64/](http://download.opensuse.org/repositories/security/SLE_12_SP2/x86_64/)
- b Download and install the package `john-<Latest version>.rpm`, for example,

<code>john-1.8.0-60.1.x86_64.rpm</code>	08-Dec-2016 14:19	4.9M	Det
<code>john-debuginfo-1.8.0-60.1.x86_64.rpm</code>	08-Dec-2016 14:19	737K	Det
<code>john-debugsource-1.8.0-60.1.x86_64.rpm</code>	08-Dec-2016 14:19	457K	Det

- c Run the seccheck again.

### 7.2 AIDE

AIDE is the Advanced Intrusion Detection Environment. It monitors changes in files with the particular purpose of detecting changes that have been caused by a malware or security breaches. Typically AIDE creates a database immediately after the system is installed.

When AIDE is running after this, it reports on changes that have taken place relative to the previous state. A configuration file controls which files and directories you wish to monitor. Documentation is included with the package.

**Note:** AIDE replaces tripwire (tm).

## 7.3 Audit Event

The Linux kernel has auditing capabilities. The user-space tools in the audit package allow an administrator to specify rules in the file `/etc/audit/audit.rules` which will force the logging of matching events. So any time that a specified program is run, or a particular file is read, the audit daemon will log that activity to the file `/var/log/audit/audit.log`. The tool `ausearch` will search that log file for specific information, and `aureport` can create various report from the log file. The use of these tools together with careful rules for `sudo` can create a highly detailed audit trail of all activities on a server.

Novell documentation for the audit package is available at on-line documentation: <https://www.suse.com/documentation/sles-12/index.html>.

## 7.4 Password Checking Tools

The built-in tools on SLES advise strong passwords. In addition, password change can be forced after a specific period of time using the `change` command or options in the `useradd` command.

Various password cracking tools are available. They can be used against the encrypted passwords stored in `/etc/shadow` to check their strength. For example, John the ripper. The Linux-PAM Guides contain very good information about the use of the PAM configuration in general, and examples of how to enforce policies regarding passwords in particular (length, number of non-alphabetic characters required, similarity to the previous password, etc).

See on-line documentation: [http://www.linux-pam.org/Linux-PAM-html/Linux-PAM\\_SAG.html](http://www.linux-pam.org/Linux-PAM-html/Linux-PAM_SAG.html)



## 8 Physical Security (Optional)

### 8.1 Editing BIOS to Disallow Booting from CDROM/Floppy/USB/Network

See the documentation for your specific BIOS. Booting from removable media allows an attacker with physical access to the machine to mount the systems' filesystems--accessing or deleting data, changing settings, or even changing passwords.

Be sure to:

- Set a BIOS password.
- Change the boot order such that the hard disk is the first.
- Physically lock the case so attacker cannot reset the BIOS.

### 8.2 Setting GRUB Password

Grub is a powerful bootloader which allows entries to be edited on the fly, but it can be a security risk.

GRUB can boot removable media or even access files on the hard disk.

To set a password in yast (see the yast **Boot Loader** module).

yast: **System > Bootloader**.

Remember to delete the 'Floppy' entry.

1. Press **enter** to login **Boot Loader Setting**.
2. Switch to the **Boot Loader Installation** tab by pressing **right arrow** on the keyboard.
3. Enable **Protect Boot Loader** with Password and then enter password.





## 9 Post Hardening Activities

### 9.1 Rebooting System

After these hardening instructions have been completed, you must reboot the system to see if everything starts up as expected and to make sure that new configurations are loaded and take effect.

### 9.2 Deploy IPWorks VNF

After the OS hardening is completed, deploy IPWorks VNF, refer to IPWorks Auto Deployment Guideline for KVM - DL380 Gen9 , Reference [7].





## Reference List

### **IPWorks Library Document**

- [1] *Trademark Information*
- [2] *Typographic Conventions*
- [3] *Glossary of Terms and Acronyms*
- [4] *IPWorks Application Components Hardening Guide*
- [5] *IPWorks OS Installation Instruction for KVM, 1/1531-AVA 901 33/3 Uen*
- [6] *IPWorks Security Management*
- [7] *IPWorks Auto Deployment Guideline for KVM - DL380 Gen9, 19/1553-AVA 901 33/3 Uen*

### **Other Reference**

- [8] [SSHD\\_CONFIG\(5\)](#)
- [9] [tcpd\(8\) Man Page](#)