

Hardening Guideline for Virtual and Cloud Deployment

Ericsson Dynamic Activation 1

OPERATION GUIDELINES

Copyright

© Ericsson AB 2017. 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

1	Introduction	1
1.1	Target Group	1
1.2	Typographic Conventions	1
2	Overview	3
3	Physical Hardening	5
3.1	Computer Room	5
3.2	System	5
4	Software Hardening	7
4.1	Performed Operating System Hardening	7
4.2	Application Software Hardening	9
4.3	Network and IP Traffic Hardening	9
5	Possible Additional Hardening Options	13
5.1	Create a Linux User	13
5.2	Time-out of SSH Sessions	13
5.3	Set Password Change Minimum Number of Days	13
5.4	Password Creation Requirement Parameters	13
6	Logging Hardening	15
7	User Handling	17
7.1	Passwords	17
8	Customer Network	19
	Reference List	21





1 Introduction

This document contains the hardening guidelines for the Ericsson Dynamic Activation (EDA) Virtual and Cloud deployment.

Note: This document should only be seen as a guideline for different hardening areas and is not to be used as an instruction for what must be done to achieve a completely hardened system.

1.1 Target Group

The target group for this document is as follows:

- System Administrator
- System Integrator

1.2 Typographic Conventions

Typographic conventions are described in the document *Library Overview*, Reference [2].

For information about abbreviations used throughout this document refer to *Glossary of Terms and Acronyms*, Reference [1].





2 Overview

For an overview of the Dynamic Activation Virtual and Cloud Deployments, see *Product Overview*, Reference [3].





3 Physical Hardening

This section contains information about hardening the physical system.

3.1 Computer Room

Place the system in an access restricted server room.

3.2 System

Make sure that the rack hosting the system is locked and that no network access points are directly accessible from outside.

Make sure to remove any keyboard/mouse/terminal from the system.





4 Software Hardening

Note: The commands throughout this section are already run in the image.

4.1 Performed Operating System Hardening

This section provides information on what has been done to harden the OS.

4.1.1 User Privileges Hardening

It is highly recommended to have a System administrator user with Superuser privileges, so that administration of the OS can be done with `sudo` instead of using `root` account (denoted with #)

For details see section **User Privileges** in *System Administrators Guide for Virtual and Cloud Deployment*, Reference [5].

4.1.2 Configure Network Time Protocol (NTP)

To ensure that log files have consistent time records, the following restrictions are set.

Additions to the `/etc/ntp.conf` file:

```
restrict default kod nomodify notrap nopeer noquery  
restrict -6 default kod nomodify notrap nopeer noquery
```

4.1.3 File System

4.1.3.1 User/Group Owner and Permissions

Authorized access to certain system files have been disabled.

The following directories or files are now ensured to have permissions 0700:

- `/etc/cron.d/`
- `/etc/cron.daily/`
- `/etc/cron.hourly/`
- `/etc/cron.monthly/`
- `/etc/cron.weekly/`



The following directories/files are now ensured to have permissions 0600:

- /etc/ssh/sshd_config
- /boot/grub2/grub.cfg

The following files are now ensured to have permissions 0600, owned by root user and group:

- /etc/crontab

chown root /etc/crontab

chgrp root /etc/crontab

chmod 0600 /etc/crontab

The following files are now ensured to have permissions 0700, owned by root user and group:

- /etc/cron.allow
- /etc/at.allow

The following files have been removed to restrict unauthorized users to run crontab jobs.

- /etc/cron.deny
- /etc/at.deny

The following directories/files are now ensured to have permissions 0755:

- /opt/glassfish3/bin

The following files and directories are ensured to be owned by root user:

- /home/bootloader/repository
- /home/dveinstaller/ma15/CXP9026214/MANIFEST
- /home/dveinstaller/ma/install_rhel_platform.py

The following directories are now ensured to be owned by root user/group and the sticky-bit has been activated. The permissions for the following directories are 1777.

- /var/.slm/
- /var/.slm/.lsysmdat/
- /var/.slmbackup/
- /var/.slmbackup/.lsysmbk



- `/var/.slmauth/`
- `/var/.slmauth/.lsysath/`
- `/usr/local/pgngn/logs/`
- `/home/bootloader/CArepository/`

4.1.3.2 Partitioning

The table below shows the partitions affected by the aforementioned options and which options are set on which partition.

Table 1 Partitioning Mount Options

	Nodev	Nosuid	Noexec
<code>/tmp</code>	X	X	
<code>/home</code>	X		
<code>/dev/shm</code>			X

The `/var/tmp` directory has been bind mounted to the `/tmp` directory. To make this change persistent the following line has been added to `/etc/fstab`:

```
/tmp /var/tmp none bind 0 0
```

The following command enables the bind on a running system:

```
# mount --bind /tmp /var/tmp
```

4.2 Application Software Hardening

Red Hat GPG keys are installed with the following command:

```
# rpm --import -vv /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-*
```

4.3 Network and IP Traffic Hardening

This section provides information on hardening procedures related to network and IP traffic.

4.3.1 SSH Configurations

The following configurations have been set for SSH:

- `Protocol 2`



SSH Protocol 2 is a more advanced and secure protocol than SSH Protocol 1 and should thus be the only protocol to be used.

- `LogLevel INFO`

LogLevel INFO specifies that only login and logout activity will be logged.

- `X11Forwarding no`

Disables the ability to login with a graphical interface.

- `IgnoreRhosts yes`

Forces users to enter a password when authenticating with SSH.

- `HostbasedAuthentication no`

This is an additional layer of protection if support for `.rhosts` is disabled in `/etc/pam.conf`

- `PermitEmptyPasswords no`

Disallows remote shell access to accounts that have no password.

- `PermitUserEnvironment no`

Prevent users from being able to set environment variables.

- `Ciphers aes128-ctr,aes192-ctr,aes256-ctr`

Only listed ciphers in Counter mode is allowed.

- `Banner /etc/issue.net`

Banner `/etc/issue.net` is empty by default, but banners are used to warn connecting users of the site's policy regarding connection.

4.3.2 SSH Connection Retries

PAMTally2 is used, which allows 10 retries instead of specifying it in the SSH configuration

4.3.3 SSH Banner Modification

Banner files such as `/etc/motd`, `/etc/issue`, and `/etc/issue.net` should not contain the lines `\m`, `\r`, `\s` or `\v`.

Replace `[COMPANY_NAME]` with the desired company name in the source file located in `/etc/puppet/modules/security/files/issue.net`



The reason for changing the source file is because the `/etc/issue.net` file is watched by puppet. It will ensure that the content of the file is the same as its source.

Default banner text included in installation:

```
[COMPANY_NAME]
```

```
This computer system including all related equipment, network devices
(specifically including Internet access), are provided only for authorized
use. All computer systems may be monitored for all lawful purposes,
including to ensure that their use is authorized, for
management of the system, to facilitate protection
against unauthorized access, and to verify security procedures,
survivability and operational security. Monitoring
includes active attacks by authorized personnel and their
entities to test or verify the security of the system.
During monitoring, information may be examined, recorded,
copied and used for authorized purposes.
All information including personal information, placed on or
sent over this system may be monitored. Uses of this system,
authorized or unauthorized, constitutes consent to monitoring of this system.
Unauthorized use may subject you to criminal prosecution.
Evidence of any such unauthorized use collected during
monitoring may be used for administrative, criminal or
other adverse action. Use of this system constitutes
consent to monitoring for these purposes.
```

Note: If a customized banner is to be used, modify the `/etc/puppet/modules/security/files/issue.net` file.

4.3.4 Firewall

The firewall service is not activated, IPTables is used to only allow access to specific services.

4.3.5 Modified Network Parameters

The following options have been added to the `/etc/sysctl.conf` file:

- These options disable send packet redirects:

```
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0
```

- These options disable ICMP redirect acceptance:

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- These options enable logging of suspicious packets:

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

The changes are applied by executing the following command:



```
# sysctl -p /etc/sysctl.conf
```




5 Possible Additional Hardening Options

This section includes information about options that have not been set but are possible to configure if needed.

5.1 Create a Linux User

It is recommended to create a non-root user for administering purposes, such as log file reading, process monitoring and more.

Follow specific instructions in section **Create Administrative User** in *System Administrators Guide for Virtual and Cloud Deployment*, Reference [5].

5.2 Time-out of SSH Sessions

The following options control the time-out of SSH sessions. These can be added to `/etc/ssh/sshd_config`:

```
ClientAliveInterval (recommended: 300)
ClientAliveCountMax (recommended: 0)
```

5.3 Set Password Change Minimum Number of Days

It is possible to set a minimum number of days before users are allowed to change their password again. Add the following line to `/etc/login.defs`:

```
PASS_MIN_DAYS 7
```

Use the following command to change this setting for an active user:

```
$ sudo chage --mindays 7 <user>
```

5.4 Password Creation Requirement Parameters

The following describes how to configure strong password enforcement.

- Set the `pam_pwquality.so` parameters as follows in `/etc/pam.d/system-auth`:
 - `password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=`



`try_first_pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password

`retry=3` - allow three tries before sending back a failure.

- Set the following in `/etc/security/pwquality.conf`:

- `minlen=14`

- Password must be 14 characters or more.

- `dcredit=-1`

- Provide at least one digit.

- `ucredit=-1`

- Provide at least one uppercase character.

- `ocredit=-1`

- Provide at least one special character.

- `lcredit=-1`

- Provide at least one lowercase character.

- Set the remember parameter to 5, to force users not to reuse their last five passwords.

Add the following line in `/etc/pam.d/system-auth`:

```
password sufficient pam_unix.so remember=5
```



6 Logging Hardening

This section describes hardening related to logging.

Messages are sent to a `syslog` (`rsyslog`) daemon running. Security related messages and events are dumped also to this `syslog` daemon.

`syslog` is rotated when it reaches a specified size, and older log files are compressed and stored.





7 User Handling

7.1 Passwords

In general:

- Do not use default passwords, but change them upon first use. This will be done by installation personnel.
- Once the system is handed over to the customer, it is the customer's responsibility to change all passwords, in line with existing security policy.
- Use strong passwords only.
 - Include numbers, symbols, upper and lowercase letters in passwords if allowed by the system
 - Password length should be around 12 to 14 characters
 - Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past), or biographical information (for example, dates, Id numbers, ancestors names or dates)

For information about strong passwords, see Reference [6].

To secure the Red Hat Enterprise Linux™ layer, the password handling could be hardened.

Action: Forced password change from default password. By avoiding the default passwords, the system becomes more secure.

Reference https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Security_Guide/index.html , Reference [7] describes how to force password change when a new account is created.

Action: Configure inactivity logout An inactivity time-out could be configured to avoid that users are still logged in to shells with no activity.

Reference https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Security_Guide/index.html , Reference [7] describes how to enable automatic logouts





8 Customer Network

For information of configuration of external firewall, see configuration document *Network Description and Configuration for Virtual and Cloud Deployment*, Reference [4].





Reference List

Ericsson Documents

- [1] *Glossary of Terms and Acronyms*, 0033-CSH 109 628 Uen
- [2] *Library Overview*, 18/1553-CSH 109 628 Uen
- [3] *Product Overview*, 1550-CSH 109 628 Uen
- [4] *Network Description and Configuration for Virtual and Cloud Deployment*, 1/1551-CSH 109 628 Uen
- [5] *System Administrators Guide for Virtual and Cloud Deployment*, 3/1543-CSH 109 628 Uen
- [6] http://en.wikipedia.org/wiki/Password_strength

Online References

- [7] *Red Hat Enterprise Linux 7 Security Guide* https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Security_Guide/index.html