

Hardening Guideline for Native 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	Network and IP Traffic Hardening	8
5	Possible Additional Hardening Options	11
5.1	Create an LDE Global User	11
5.2	Time-out of SSH Sessions	11
5.3	Set Password Change Minimum Number of Days	11
5.4	Limit Password Reuse	11
5.5	Password Creation Requirement Parameters	12
6	Logging Hardening	13
7	User Handling	15
7.1	Passwords	15
8	Connectivity	17
8.1	MML Interface	17
8.2	CLI/Telnet Interface	17
9	Customer Network	19
	Reference List	21





1 Introduction

This document contains the hardening guidelines for the Ericsson Dynamic Activation (EDA) GEP3, and GEP5 blade configurations, based on Component Based Architecture (CBA).

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 native configurations, 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

The system consists of GEP3, SCX, CMX or GEP5, SCX, CMX hardware components.

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 have 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 Native Deployment*, Reference [6].

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`:

```
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/grub/menu.lst`

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

- `/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/directories are now owned by root user and/or group:

- `/cluster/rpms/`
- `/opt/dve/bin/`

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

- `/opt/glassfish3/bin`

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

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

4.2 Network and IP Traffic Hardening

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

4.2.1 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.

4.2.2 SSH Connection Retries

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

4.2.3 Access via SSH

Access via SSH is limited and is solved with `login.allow` in LDE. For details, refer to Reference [8].

4.2.4 SSH Banner Modification

Banner files such as `/cluster/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 `/home/dveadm/config/legalbanner`

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, see specific instructions in Reference [8].

4.2.5

Firewall

SuSEfirewall12 is not activated, IPTables is used to only allow access to specific services.



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 an LDE Global User

It is recommended to create a global LDE 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 Native Deployment*, Reference [6].

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)
```

Note: Configuration is lost on reboot.

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:

```
# chage --mindays 7 <user>
```

5.4 Limit Password Reuse

Setting the remember parameter to 5 forces users not to reuse their last five passwords.

Use the following command to set the remember parameter to 5:

```
# pam-config -a --pwhistory --pwhistory-remember=5
```



5.5 Password Creation Requirement Parameters

Use the following command to configure a stronger password enforcement:

```
# pam-config -a --cracklib --cracklib-retry=3 --cracklib-minlen=14 --cracklib-dcredit=-1 --cracklib-ucredit=-1 --cracklib-ocredit=-1 --cracklib-lcredit=-1
```

The following settings are used in the above command:

- `cracklib-retry=3`
Allow three tries before sending back a failure.
- `cracklib-minlen=14`
Password must be 14 characters or more.
- `cracklib-dcredit=-1`
Provide at least one digit.
- `cracklib-ucredit=-1`
Provide at least one uppercase character.
- `cracklib-ocredit=-1`
Provide at least one special character.
- `cracklib-lcredit=-1`
Provide at least one lowercase character.



6 Logging Hardening

This section describes hardening related to logging.

Messages are sent to a `syslog` (`rsyslog`) daemon running in the System Controllers (SC). 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 [7].

7.1.1 CMX Router

No hardening software action is needed on the CMX. This since the CMX routers are only accessible from the DMXC.

7.1.2 BSP

For BSP hardening, refer to **BSP Hardening Guideline**, Reference [5].

7.1.3 LDEwS

To secure the Linux™ Distribution Extensions with SUSE (LDEwS) layer, the password handling could be hardened.

Action: Forced password change from default password

By avoiding the default passwords, the system becomes more secure. The Reference [8] 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. The Reference [8] describes how to configure inactivity logout for `bash` and `tcsh`.



8 Connectivity

8.1 MML Interface

The recommendation is to use the secured MML interface and to block the unsecure MML port in the firewall.

8.2 CLI/Telnet Interface

The recommendation is to use the secured CLI/Telnet interface and to block the unsecure CLI/Telnet port in the firewall.





9 Customer Network

For information of configuration of external firewall, see configuration document for Native deployment, using GEP3 or GEP5 blades, *Network Description and Configuration for Native 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 Native Deployment*, 2/1551-CSH 109 628 Uen
- [5] *BSP Hardening Guideline*, 7/1553-APP 111 01 Uen
- [6] *System Administrators Guide for Native Deployment*, 1/1543-CSH 109 628 Uen
- [7] http://en.wikipedia.org/wiki/Password_strength
- [8] *LDE Management Guide*, 1/1553-CAA 901 2978/1 Uen