

CSCF Hardening Guideline

Call Session Control Function

USER GUIDE

Copyright

© Ericsson AB 2016–2018. 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

1	Introduction	1
1.1	Prerequisites	1
2	Hardening Guidelines	3
2.1	General Information about Product Hardening	3
2.2	Hardening during Product Development	4
2.3	Hardening during Service Delivery	4
2.4	Operating System Hardening	4
2.5	Application Software Hardening	9
2.6	Operation and Maintenance	9
2.7	Network and IP Traffic-Related Hardening	11
2.8	Logging	14
2.9	Miscellaneous	15
2.10	Post-Work	15





1 Introduction

This document describes the hardening procedure of the Call Session Control Function (CSCF).

This includes the following:

- General information about hardening of the product

This is useful for understanding the purpose of product hardening and the scope of product hardening.
- A list of the hardening activities performed during the product development phase (pre-hardening report)
- Instructions on how to perform the remaining hardening activities during service delivery integration phase

Local policy requirements for hardening are out of scope of this document.

Target Group

This document is intended for service delivery integration engineers and system and security administrators.

1.1 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedures in this document.

1.1.1 Documents

This document references the following documents:

- *Audit Information*
- *CSCF Security User Guide*
- *Ericsson Alarm Interface*
- *Handling Alarms*
- *User Management*



1.1.2 Conditions

Before starting these procedures, ensure that the following conditions are met:

- The CSCF application is installed.
- Security and hardening activities within the site infrastructure are already performed.

Note: The security and hardening activities to be performed in the site infrastructure are outside the scope of this document.



2 Hardening Guidelines

This section describes the hardening of the product. Part of it is performed during product development, and the product hardening is completed during service delivery.

2.1 General Information about Product Hardening

The CSCF can take different roles in the network, as follows:

- Interrogating Call Session Control Function (I-CSCF) – As the entry point to the home network, it provides dynamic allocation of the Serving Call Session Control Function (S-CSCF).

I-CSCF also serves as Breakout Gateway Control Function (BGCF). The BGCF is used primarily to select an outgoing gateway for a SIP request addressed to a telephone number.

- Serving Call Session Control Function (S-CSCF) – Performs session control services for the UE by providing subscriber registration, multimedia session invocation, modification, clearing, routing, and redirecting.

S-CSCF also serves as BGCF. The BGCF is used primarily to select an outgoing gateway for a SIP request addressed to a telephone number.

- Emergency Call Session Control Function (E-CSCF) – Handles emergency calls in a standardized way.

E-CSCF also serves as BGCF. The BGCF is used primarily to select an outgoing gateway for a SIP request addressed to a telephone number.

- Break-in Control Function (BCF) – Gives the possibility for users connected to other networks to execute originating IMS services.
- Emergency Access Transfer Function (EATF) – performs anchoring of VoLTE emergency calls. EATF also enables the access network transfer of VoLTE emergency calls from a PS to CS access network.

In this document, it is assumed that the CSCF is deployed in standalone configurations. If the CSCF is deployed in a collocated node configuration as shown in Figure 1, the same hardening is applied. Figure 1 outlines the CSCF external interfaces and to what possible network configuration these interfaces belong. All the traffic between different networks is to be separated and must be assigned different VIP External Networks which are connected to different VIP Routers with built-in firewall functionality, refer to *CSCF VNF Network Connectivity Overview*. The discussion in this document is based on this assumption.

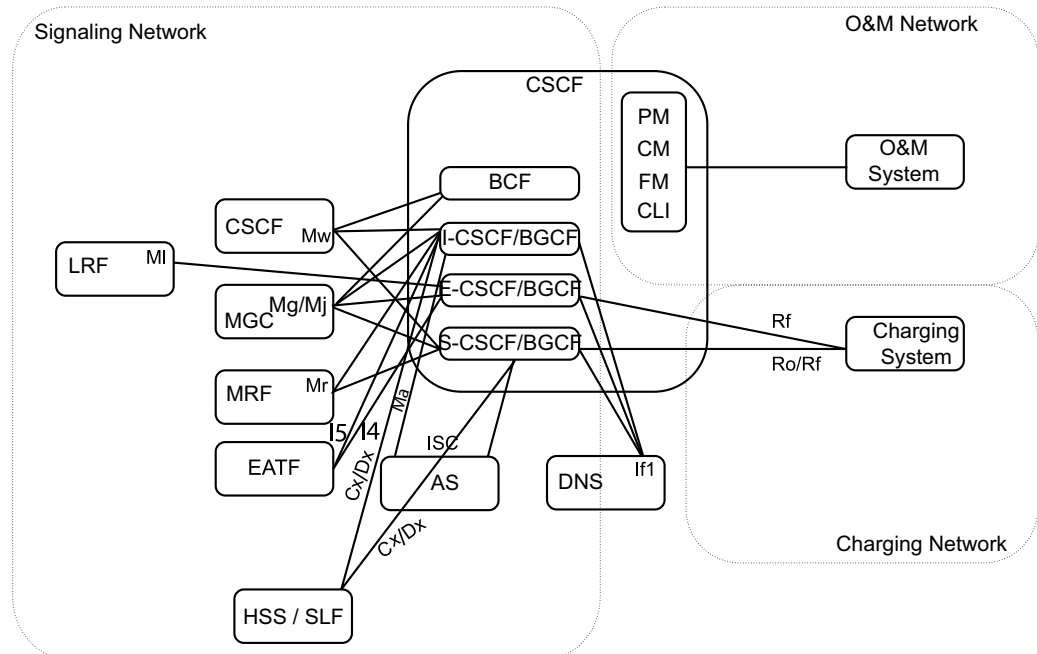


Figure 1 Possible Network Configuration

2.2 Hardening during Product Development

Not applicable

2.3 Hardening during Service Delivery

Not applicable

2.4 Operating System Hardening

This section describes hardening for operating system.

2.4.1 Operating System Configuration

This section describes the hardening for operating system configuration.



2.4.1.1 Create Emergency User

At least one emergency user must be configured in the system. When no LDAP server is accessible, an emergency user can log on to the system to perform emergency management activities.

To configure a new emergency user, use the Linux[®] command line to create a local user and add it to group `com-emergency`:

1. Log on to one of the system controllers as root:

```
ssh -l root <address>
```

2. Add a user account:

```
useradd -G com-emergency <new user account>
```

```
lde-global-user -u <new user account>
```

By specifying option `lde-global-user -u <new user account>`, the LDEfR adds the specified user to all nodes in the cluster.

A new account is created according to the defaults of `/etc/default/useradd`. The account is added to the `com-emergency` group.

3. Set password for the user account:

```
passwd <new user account>
```

Note: The system prompts the user for a password and asks the user to repeat the selected password. For more information about password change and aging, see Section 2.4.1.10 Force Password Change and Aging on page 8.

4. Allow the user account to log on to all nodes in the cluster by editing file `login.allow`.

- a. Open `login.allow` file in the vi editor.

- b. Add the user account to file `login.allow`:

```
vi /cluster/etc/login.allow
```

- c. Enter the user account on a new line:

```
<new user account> all
```

5. Log off from the system controller:

```
Exit
```

Create separate accounts for each emergency user.

2.4.1.2 Avoid Using Shared Accounts

Account sharing is a bad security practice and major security liability which must be avoided. Always assign user personal accounts instead of shared or generic user accounts.

2.4.1.3 Prevent Remote root Logon Through SSH

Remote logon for root user is enabled by default.

To disable remote logon for root user:

1. Add the line `ssh.rootlogin all off` to the `/cluster/etc/cluster.conf` file.
2. Reload the configuration using the command `cluster config -a -r` on one of the controllers.

2.4.1.4 Change Password for root User

Since the predefined password for the root user is known by many persons, it must be changed. Use command:

```
passwd root
```

The system prompts the user to enter a password and then asks the user to repeat the selected password.

2.4.1.5 Password-less Logon

Password-less is used to log on to the CSCF without entering a pass-phrase or a password. By default, a pass-phrase and a password are required when logging on to the CSCF. Configuring password-less logon is optional. For details, refer to *CSCF Configuration Management*.

2.4.1.6 Delete Unused Local Linux Accounts

Audit the node to make sure all user accounts created are required and accounted for. Remove any user accounts that are not required.



Attention!

Risk of system malfunction or traffic disturbance.

Do not delete the default users created by the system.



2.4.1.7 Change Logon Banner

By default, no information is provided to the user when logging on using a Command-Line Interface (CLI) based shell including SSH interface. However, the system provides the file `/cluster/etc/motd`, which allows a text message to be created and later displayed when the user logs on to the system successfully. The same message is displayed to all users when performing a logon on system controllers.

If banner information is required for the SSH interface before a logon screen, edit file `/cluster/etc/issue.net` with banner information.

2.4.1.8 Enable Inactivity Timer for Logon

The inactivity timer is set to 600 seconds by the system.

2.4.1.9 Enable Strong Password Enforcement

Password enforcement is enabled by default. The user `root` is not following these rules.

The following rules are enforced:

- Passwords must be at least eight characters long.
- Passwords must contain at least three of the following elements:
 - At least one lower case alpha character.
 - At least one upper case alpha character.
 - At least one numeric character.
 - At least one special character.
- Passwords must have no more than three of the same characters used consecutively.
- No real names or words, either with numbers in front or at the tail.
- Passwords must not be a repeat or the reverse of the associated user ID.
- Each new logon password must differ from the previous password. The degree of difference is at least three character positions.
- Each node supports a password history to prevent password reuse. At least five unique new passwords must be associated with a user account before an old password can be reused.



2.4.1.10 Force Password Change and Aging

2.4.1.10.1 Account and Password Aging

When a user account is created, no account or password aging are applied by default. However, by using standard Linux tool, `chage`, it is possible to set up both account and password aging. It is, for example, possible to set up the maximum days a password is valid, how many days before expiration a warning message is displayed to the user at logon, and for how many days an account can have an expired password before the account is inactivated. Table 1 gives some hints of good practice values when defining account and password aging. The values are recommendations and can be changed at any time when suitable.

Table 1 Account and Password Aging

Parameter	Value
Account expire date	-1 (disabled)
Account inactive date	30
Minimum number of days before password can be changed	0
Maximum number of day before password must be changed	90
Number of days before password expiring a warning message is given to user (at logon)	7

To apply the values in Table 1 or a user, issue the following command:

```
chage <user name> --mindays 0 --maxdays 90 --expiredate -1  
--inactive 30 --warndays 7
```

The `chage` (1) man page gives more details about syntax and available options.

2.4.1.10.2 Force Password Change

When a user account is created or reactivated, it can be given a default password that must be changed the first time the user logs on to the system. To force the user to change the password, issue the following command after the user account has been created or reactivated:

```
passwd -e <user name>
```

The `passwd` (1) man page gives more details of available options.



2.4.1.11 Configure User Account Inactivity

For information about the inactivity timer for user accounts, refer to section *Inactivity timer for User Accounts* in *LDE Management Guide*.

2.5 Application Software Hardening

This section describes the hardening for the application software.

2.5.1 Application Software Installation

This section describes the hardening for the application software installation.

2.5.1.1 Get Latest Software Version and Patches

It is highly recommended to get the latest available software version of the CSCF. This ensures that the latest security patches are added after initial delivery.

2.5.2 Application Software Configuration

2.5.2.1 System Function Configuration

Some of the system functions that are configurable over NBI can be configured with different levels of security. SNMP targets are preferably configured with the most secure option, SNMPv3 and LDAP are configured with the strongest possible ciphers. For details on LDAP Authentication and Local Authorization, refer to *User Management*.

2.6 Operation and Maintenance

This section describes the hardening for the operation and maintenance.

2.6.1 System Access Control, Authentication, and Authorization

2.6.1.1 Disable-Serial

The disable-serial parameters are shown in Table 2.



Table 2 Disable-Serial (for LDEwS)

Syntax	disable-serial <value>	
Description	Disables the serial console for the whole cluster. In contrast to default-output, which sets what the system is to default to, disable-serial removes the serial console option completely.	
Options	<value>	Either on to use serial console or off to disable serial console.
Examples	disable-serial on disable-serial off	

2.6.1.2 Disable Root Access Through NBI

Root access through the NBI is disabled by default.

2.6.2 Password and Logon Control

This section describes hardening for password and logon control.

2.6.2.1 Passwords

Do not use default passwords, change them upon first use.

Password-less is used to log on to the CSCF without entering a pass-phrase or a password. By default, a pass-phrase and a password are required when logging on to the CSCF. Configuring password-less logon is optional. For details, refer to *CSCF Configuration Management*.

2.6.2.2 Configure CLI Inactivity Timer

The CLI inactivity timer automatically terminates a session after a CLI user is idle for a certain period. It is configurable and the default value is 120 seconds.

To change the CLI connection time-out, modify the CLI agent configuration file `/cluster/storage/system/config/com-apr9010443/lib/comp/libcom_cli_agent.cfg` and change the value of the element `<connectionTimeout>`:



```
<?xml version="1.0" encoding="utf-8"?>
<comCfg>
  <component>
    <name>ComCliAgent</name>
    <version>1</version>
    ...
    <ComCliAgent>
    ...
      <connectionTimeOut>
        <Add a value in seconds here>
      </connectionTimeOut>
    ...
    </ComCliAgent>
  </component>
</comCfg>
```

Reload COM/NBI to deploy the modified configuration.

2.6.2.3 Configure Legal Message for CLI Logon

It is a common corporate policy to display a legal message when a user logs on through the CLI.

To configure the legal message, modify the CLI agent configuration file `/cluster/storage/system/config/com-apr9010443/lib/comp/libcom_cli_agent.cfg` and assign the desired message to the element `<IntroductoryMessage>`:

```
<?xml version="1.0" encoding="utf-8"?>
<comCfg>
  <component>
    <name>ComCliAgent</name>
    <version>1</version>
    ...
    <ComCliAgent>
    ...
      <IntroductoryMessage>
        <Add a legal message here>
      </IntroductoryMessage>
    </ComCliAgent>
  </component>
</comCfg>
```

Reload COM/NBI to deploy the modified configuration.

2.7 Network and IP Traffic-Related Hardening

This section describes the hardening for the network and IP traffic-related hardening.



2.7.1 Host-Based Firewall Configuration

This section describes hardening for host-based firewall configuration.

2.7.1.1 SSH Restriction to a Specific Network

The SSH parameters are shown in Table 3. The iptables parameters are shown in Table 4.

Table 3 SSH Parameters

Syntax	<code>ssh <target> <network></code>	
Description	Restrict SSH to listen to a specific network. This parameter can be defined multiple times if SSH listens to more than one network. Note: if <code>ssh</code> is not defined for a blade, no restriction on SSH is made, meaning it listens to all available interfaces.	
Options	<code><target></code>	Target blades.
	<code><network></code>	Name of the network that SSH listens to.
Examples	<code>ssh payload internal</code>	
Exceptions	If the <code>ssh</code> keyword is defined for a network, SSH cannot be used towards movable IPs on that network. If SSH access to movable IPs is required, remove all <code>ssh</code> parameters and <code>iptables</code> used to restrict SSH traffic.	



Table 4 iptables Parameters

Syntax	iptables <target> <command>	
Description	Defines a rule in iptables. Rules are run in the order specified in this configuration.	
Options	<target>	Target blades.
	<command>	Specifies the parameters that must be passed to iptables. This can be any parameter accepted by iptables, see man page of iptables(8) for more information.
Examples	<p>On all nodes, drop packets destined from source address 10.0.0.1:</p> <pre>iptables all -A INPUT -s 10.0.0.1 -j DROP</pre> <p>On all nodes, accept SSH traffic destined for the 192.168.0.0/24 network and drop all other SSH traffic:</p> <pre>iptables all -A INPUT -p tcp --dport 22 -d 192.168.0.0/24 -j ACCEPT</pre> <pre>iptables all -A INPUT -p tcp --dport 22 -j DROP</pre>	

2.7.2 Securing Services

This section describes the hardening for securing services.

2.7.2.1 Disable Internal Services on External Networks

The iptable must be configured to block NFS against to be accessed from external networks.

It is not possible to mount the NFS share over any network apart from the internal network. The services on the External Network must be blocked and the following iptables rules must apply, one for each network:

```
iptables -A INPUT -p <protocol> --match multiport
--destination-port <ports_to_be_blocked> -j REJECT
--reject-with icmp-port-unreachable -s <external-network>
```

Where <protocol> is {**tcp**, **udp**}, <ports_to_be_blocked> are 22, 111, 2049, and <external-network> is any External Network that is configured on the blade. Repeat the command for each protocol and each network.

These changes are not persistent. Therefore, they must be redone after each reboot of a controller.

Examples of how to configure iptables are shown in Example 1 and Example 2:

```
iptables control -A INPUT -p tcp --match multiport
--destination-port 22,111,2049 -j REJECT
--reject-with icmp-port-unreachable -d 10.0.0.0/24
```

Example 1 Configure iptables Example 1

```
iptables control -A INPUT -p udp --match multiport
--destination-port 22,111,2049 -j REJECT
--reject-with icmp-port-unreachable -d 10.0.0.0/24
```

Example 2 Configure iptables Example 2

2.7.2.2 Enforce Security of OAM Protocols

The CSCF provides SSH subsystem executables to allow SSH-based access to the NETCONF and CLI NBIs independently.

File management is using SFTP.

SNMP v3 provides important security features that are lacking in SNMP v1/v2, including authentication, confidentiality, and integrity. It is recommended to use only SNMP v3 on the NBI. For details regarding the configuration of SNMP v3, refer to *Handling Alarms* and *Ericsson Alarm Interface*.

Avoid weak hashing algorithms, such as MD5, when signing the operator certificates. This prevents X.509 certificate signature collision that can happen with weak hashing functions.

2.8 Logging

This section describes the hardening for the logging.

2.8.1 Auditing

For information about the audit log, refer to *Audit Information*.

2.8.1.1 Enable Linux Auditing Framework

Full personal accountability entails the ability to log watch O&M actions are taken by users logged on to the system. This is accomplished through enabling the Linux auditing framework. The Linux auditing framework is enabled by default.



2.9 Miscellaneous

This section describes other activities to be performed during hardening.

2.9.1 Reboot Cluster

To get all the file changes to work, a total cluster reboot is required:

1. Create a backup of the cluster.
2. Reboot the cluster:

```
cluster reboot -a
```

2.9.2 Remove Development and Installation Scripts and Tools

All installation scripts and tools are to be removed after installation is completed.

2.9.3 Create System Backup

After the hardening activities have been performed, create a backup of the system. It is also recommended uploading the backup to external storage.

2.10 Post-Work

This section describes the post-work.

2.10.1 Perform Regression or Validation Test

Perform a regression or validation test to check that the system performs as expected.

2.10.2 Fill in the CSCF Hardening Checklist

Fill in the CSCF hardening checklist as shown in Table 5 and archive it as a reference.



Table 5 CSCF Hardening Checklist

Hardening Area	Hardening Activity	Check Mark	Comments
	Create emergency user		
	Avoid using shared accounts		
	Prevent remote root logon through SSH		
	Change password for root user		
	Password-less logon		
	Delete unused local Linux [®] accounts		
	Change logon banner		
	Enable inactivity timer for logon		
	Enable strong password enforcement		
	Force password change and aging		
	Configure User Account Inactivity		
Software Version Control	Get latest software version and patches		
Operation and Maintenance	Configure CLI inactivity timer		
	Configure legal message for CLI logon		
Network and IP Traffic-Related Hardening	Disable internal services on external networks		
	Enforce security of OAM protocols		
Logging	Enable Linux auditing framework		



Table 5 CSCF Hardening Checklist

Hardening Area	Hardening Activity	Check Mark	Comments
	Reboot cluster		
	Remove development and installation scripts and tools		
	Create system backup		
	Perform regression or validation test		
	Archive this checklist when ready		
CSCF product version:			
Date when hardening activities were completed:			
Hardening activities performed by:			