

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 | Understanding Hardening in the CSCF | 1 |
| 1.2 | Prerequisites | 3 |
| 2 | Hardening Guidelines | 4 |
| 2.1 | Hardening during Product Development | 4 |
| 2.2 | Hardening during Service Delivery | 4 |
| 2.3 | Operating System Hardening | 4 |
| 2.4 | Application Software Hardening | 8 |
| 2.5 | Operation and Maintenance Hardening | 8 |
| 2.6 | Network and IP Traffic-Related Hardening | 10 |
| 2.7 | Logging | 12 |
| 2.8 | Miscellaneous | 12 |
| 3 | CSCF Hardening Checklist | 13 |





1 Introduction

1.1 Understanding Hardening in the CSCF

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).

The 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.

The 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.

The 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 user guide, it is assumed that the CSCF is deployed in standalone configurations. If the CSCF is deployed in a collocated node configuration, the same hardening is applied.

All the traffic between different networks must be separated and assigned to different VIP External Networks which connect to different VIP Routers with built-in firewall functionality. For more information, see [CSCF VNF Network Connectivity Overview](#). This user guide is based on this assumption.

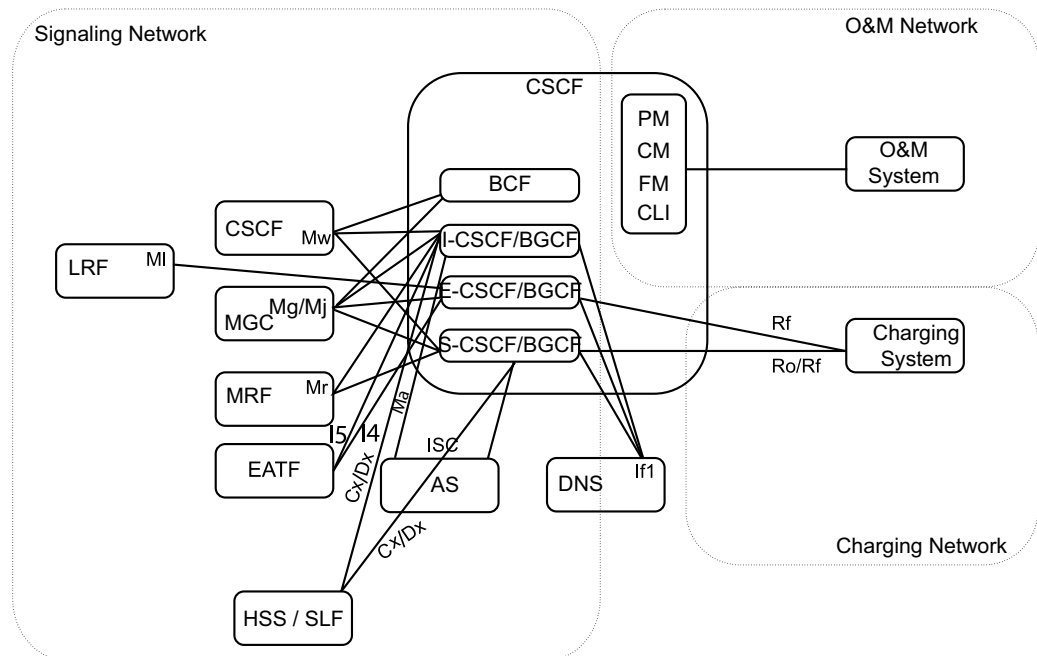


Figure 1 CSCF External Interfaces and Possible Network Configuration

This user guide contains the following hardening tasks:

- Operating System Hardening:
 - Section 2.3.1 Create Emergency User on page 4
 - Section 2.3.2 Harden the Root User on page 5
 - Section 2.3.3 Harden the User Accounts on page 6
 - Section 2.3.4 Harden Logging on to the CSCF on page 6
 - Section 2.3.5 Harden the Passwords on page 7
- Application Software Hardening:
 - Section 2.4.1 Harden the Software on page 8
- Operation and Maintenance Hardening:
 - Section 2.5.1 Harden System Access Control, Authentication, and Authorization on page 8
 - Section 2.5.2 Harden Password and Logon Control on page 9
- Network and IP Traffic-Related Hardening:
 - Section 2.6.1 Configure the Host-Based Firewall on page 10
 - Section 2.6.2 Harden the Securing Services on page 11
- Logging:
 - Section 2.7.1 Observe Logging Information on page 12



- Section 2.8.1 Complete the Hardening of the CSCF on page 12

1.2 Prerequisites

- This user guide refers to the following documents:

- Audit Information
- Create Backup
- CSCF Configuration Management
- CSCF VNF Network Connectivity Overview
- Ericsson Alarm Interface
- Handling Alarms
- LDE Management Guide
- User Management

- No tools are required.

- The following conditions must apply:

- The CSCF application is installed.
- All the traffic between different networks is separated and assigned to different VIP External Networks which connect to different VIP Routers with built-in firewall functionality.

For more information, see [CSCF VNF Network Connectivity Overview](#).

- 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 user guide.

- Local policy requirements for hardening are out of scope of this user guide.
- The user is a service delivery integration engineer or system and security administrator.



2 Hardening Guidelines

2.1 Hardening during Product Development

Not Applicable

2.2 Hardening during Service Delivery

Not Applicable

2.3 Operating System Hardening

2.3.1 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:

Steps

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 2.3.5 Harden the Passwords on page 7.



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.

2.3.2

Harden the Root User

Steps

1. Disable remote logon for the root user through SSH:
 - a. Open the `/cluster/etc/cluster.conf` file, using, for example, vi:

```
vi /cluster/etc/cluster.conf
```
 - b. Add the line `ssh.rootlogin all off` to the `/cluster/etc/cluster.conf` file.
 - c. Close the `/cluster/etc/cluster.conf` file.
 - d. Log on to one of the controllers.
 - e. Reload the configuration:

```
cluster config -a -r
```
 - f. Log off from the controller.

Remote logon for root user is enabled by default.

2. Change the predefined password for the root user:
 - a. Execute the following command:

```
passwd root
```
 - b. When prompted by the system, enter a new password.



- c. When prompted by the system, repeat the selected password.

2.3.3 Harden the User Accounts

Steps

1. Always assign user-personal accounts instead of shared or generic user accounts.
2. Delete unused local Linux® Accounts:
 - a. Audit the node to make sure all user accounts created are required and accounted for.
 - b. 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.

2.3.4 Harden Logging on to the CSCF

Steps

1. Configure password-less logon:

Follow the procedure in Section Configure Password-Less Logon in [CSCF Configuration Management](#).

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.

2. Change the logon banner:

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

This 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 logging on to the System Controllers.

3. Observe the following inactivity timer settings:

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



For information about the inactivity timer for user accounts, see section Inactivity timer for User Accounts in [LDE Management Guide](#).

2.3.5

Harden the Passwords

Steps

1. Observe the following rules for 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. Force the user to change the password after the user account has been created or reactivated:

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

For more information about the `passwd` available options, see the `passwd(1)` man page.

3. Create an account and password aging rule for a user account:

```
chage <user name> --mindays <mindays_value> --maxdays
<maxdays_value> --expiredate <expiredate_value> --inactive
<inactive_value> --warndays <warndays_value>
```

The following is an example, based on the recommended account and password aging settings:

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

The recommended values can be changed when needed.



For more information about the chage syntax and available options, see the `chage(1)` man page.

Table 1 Recommended Account and Password Aging Settings

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

2.4 Application Software Hardening

2.4.1 Harden the Software

Steps

1. Make sure to get the latest available software version of the CSCF.

This ensures that the latest security patches are added after initial delivery.
2. Configure the system functions that are configurable over the NBI:
 - a. Configure the SNMP targets with the most secure option.
 - b. Configure the SNMPv3 and LDAP with the strongest possible ciphers.

For details on LDAP Authentication and Local Authorization, see [User Management](#).

2.5 Operation and Maintenance Hardening

2.5.1 Harden System Access Control, Authentication, and Authorization

Steps

1. Remove the serial console option:

```
disable-serial off
```



This disables the serial console for the whole cluster. In contrast to `default-output`, which sets the system to the default configuration, `disable-serial` removes the serial console option completely.

2. Observe the following default setting for root access through the NBI:

Root access through the NBI is disabled by default.

2.5.2

Harden Password and Logon Control

Steps

1. Change the default password or configure password-less logon:
 - a. To force a user to change the password upon first use, follow the steps in Section 2.3.4 Harden Logging on to the CSCF on page 6.
 - b. To configure password-less logon, follow the procedure in Section Configure Password-Less Logon in *CSCF Configuration Management*.

2. If needed, change the default value of the CLI inactivity timer:

The CLI inactivity timer automatically ends a session after a CLI user is idle for a certain period. The default value is 120 seconds.

- a. Open the CLI agent configuration file `/cluster/storage/system/comfig/com-apr9010443/lib/comp/libcom_cli_agent.cfg`.
- b. 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>
```

- c. Reload COM/NBI to deploy the modified configuration.
3. If needed, configure the legal message for CLI logon:

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



- a. Open the CLI agent configuration file `/cluster/storage/system/config/com-apr9010443/lib/comp/libcom_cli_agent.cfg`.
- b. Change the value of 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>
```

- c. Reload COM/NBI to deploy the modified configuration.

2.6 Network and IP Traffic-Related Hardening

2.6.1 Configure the Host-Based Firewall

Steps

1. Restrict the SSH to listen to a specific network:

```
ssh <target_blades> <network_name_that_SSH_listens_to>
```

Note: If the `ssh` 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 `ssh` parameters and `iptables` used to restrict SSH traffic.

The following is an example:

```
ssh payload internal
```

This parameter can be defined multiple times if SSH listens to more than one network. If `ssh` is not defined for a blade, no restriction on SSH is made, meaning it listens to all available interfaces.

2. Define all necessary `iptables` rules:

```
iptables <target_blades> <command>
```

The following is an example where, on all nodes, packets are dropped that are destined from source address `10.0.0.1`:



```
iptables all -A INPUT -s 10.0.0.1 -j DROP
```

The rules are run in the order specified in this configuration.

For more information and the available parameters, see the `iptables(8)` man page.

2.6.2 Harden the Securing Services

Steps

1. Configure iptables 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.

- a. Apply the following iptables rules for each network:

```
iptables -A INPUT -p tcp --match multiport
--destination-port 22,11,2049 -j REJECT --reject-with
icmp-port-unreachable -s <external-network>
```

```
iptables -A INPUT -p udp --match multiport
--destination-port 22,11,2049 -j REJECT --reject-with
icmp-port-unreachable -s <external-network>
```

The following are examples:

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

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

Note: These changes are not persistent: redo them after each reboot of a controller.

2. Observe the following information about the 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. Only use SNMP v3 on the NBI. For details regarding the configuration of SNMP v3, see [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.

2.7 Logging

2.7.1 Observe Logging Information

Steps

1. Observe the following information about logging:
 - For information about the audit log, see [Audit Information](#).
 - Full personal accountability, the ability to log O&M actions that are taken by users that are logged on to the system, is accomplished through enabling the Linux® auditing framework. The Linux auditing framework is enabled by default.

2.8 Miscellaneous

2.8.1 Complete the Hardening of the CSCF

Steps

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

Follow the instruction in [Create Backup](#).
 - b. Upload the backup to an external storage unit.
 - c. Reboot the cluster:

```
cluster reboot -a
```
2. Check that the system performs as expected by doing a regression or validation test.
3. Remove all installation scripts and tools after the installation is completed.



3 CSCF Hardening Checklist

Use the following checklist when completing the hardening procedure and archive it as a reference if needed.

Table 2 CSCF Hardening Checklist

| Hardening Area | Hardening Activity | Check Mark | Comments |
|------------------------------------------------|-----------------------------------------------------------------|------------|----------|
| Operating System | Create emergency user | | |
| | Harden the root user | | |
| | Harden the user accounts | | |
| | Harden logging on to the CSCF | | |
| | Harden the passwords | | |
| Software Version Control | Harden the software | | |
| Operation and Maintenance | Harden system access control, authentication, and authorization | | |
| | Harden password and logon control | | |
| Network and IP Traffic-Related Hardening | Configure the host-based firewall | | |
| | Harden the securing services | | |
| Logging | Observe the logging information | | |
| Miscellaneous | Complete the hardening of the CSCF | | |
| CSCF product version: | | | |
| Date when hardening activities were completed: | | | |
| Hardening activities performed by: | | | |