

Emergency Recovery Procedure for CSCF

Call Session Control Function

EMERGENCY RECOVERY

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	Recovery Scenarios	5
2.1	Disturbances or Stoppage in Traffic Processing	5
2.2	Worst Case Scenario	6
3	Recovery Procedures	7
3.1	Disturbances or Stoppage in Traffic Processing	7
3.2	Worst Case Procedure	25
4	Report Problems	27
4.1	Problem Solved	27
4.2	Consult Next Level of Support	27





1 Introduction

This document gives an overview of the emergency recovery tasks to be performed on the Call Session Control Function (CSCF).

Typically, an emergency procedure is required for conditions that make communication or normal management and alarm handling impossible. In a worst case scenario, a procedure is required to restore the node. Emergency in this document refers to the situations described in Section 2 on page 5.

Note: Some of the emergency recovery procedures refer to the procedures to be followed in other documents. If printing this document to follow the procedures, also print the referred documents.

The system is assumed to have been in a fully working state before the problems started. Therefore no troubleshooting procedures that relate to faulty configuration or incorrect software version are explained. For this type of information, refer to [CSCF Troubleshooting Guideline](#).

Some steps that have been identified as risky from an In-Service Performance (ISP) point of view are avoided in this document. When such steps are necessary, contact the next level of support, see Section 4.2 Consult Next Level of Support on page 27. This way there are at least two different levels of support involved before making a risky decision.

1.1 Prerequisites

This section states the prerequisites for performing the emergency recovery procedures.

1.1.1 Documents

Before starting this procedure, ensure that the following information or documents are available:

- Information as, for example, node name, software version, platform, operating system, hypervisor, and hardware.
- Information about how to collect data and log files, refer to [Data Collection Guideline for CSCF](#).
- Information on how to make backup and restore procedures, refer to the following documents:
 - [Create Backup](#)
 - [Restore Backup](#)



- Information on how to perform system health check, refer to [CSCF Health Check](#).
- CSCF alarm description, refer to [CSCF Alarm List](#).

1.1.2

Tools

The following tools are required:

- Refer to [Ericsson Command-Line Interface User Guide](#) and [Ericsson NETCONF Interface](#) through which the following can be performed:
 - Configuration Management
 - Software Inventory
 - Software Backups
 - Software Upgrades
 - Fault Management
- Northbound Interface (NBI) for Alarms and Notifications.
 - View alarms and notifications
- CSCF Health Check script
- Tracing:
 - UserTrace
For more information, refer to [CSCF User Tracing](#).
 - NetTrace
For more information, refer to [CSCF Network Tracing](#).
 - AppTrace
For more information, refer to [CSCF AppTrace User Guide](#).

1.1.3

Conditions

Before starting this procedure, get familiar with the following information types that can be issued and also helps with identifying scenarios and recovery procedures:

- CSCF-related issues:
 - Disturbances or stoppage in traffic processing



— Platform-related issues:

- Disturbances or stoppage in traffic handling
- Disturbances or stoppage in provisioning
- The system is no longer single point of failure safe
- The CSCF system is down

The scope of the document is to cover CSCF-related issues in a virtual environment. For general Virtual Network Function (VNF) issues, refer to [Emergency Recovery Procedure](#) or contact the next level of support. For more information on what procedure to follow for each scenario, see Section 2 on page 5.





2 Recovery Scenarios

This section describes different recovery scenarios, as shown in Table 1.

Table 1 Scenarios for Recovery

Scenario	Conditions	Recovery Procedure
Disturbances or stoppage in traffic processing, with details in Section 2.1 Disturbances or Stoppage in Traffic Processing on page 5.	<ul style="list-style-type: none"> • Session Initiation Protocol (SIP) requests are rejected. • Diameter requests are rejected. • Reduced Capacity because of closed port on payloads. 	See Section 3.1 Disturbances or Stoppage in Traffic Processing on page 7.
Disturbances or stoppage in Traffic Handling	<ul style="list-style-type: none"> • IP traffic not working properly. • Stream Control Transmission Protocol (SCTP) traffic not working properly. 	The issues are related to platform, consult next level of support.
Disturbances or stoppage in provisioning	<ul style="list-style-type: none"> • Provisioning function not working properly. • Backup function not working properly. 	The issues are related to platform, consult next level of support.
System is no longer single point of failure safe	System lost its redundancy for a vital function.	The issues are related to platform, consult next level of support.
Worst case scenario, with details in Section 2.2 Worst Case Scenario on page 6.	The CSCF system is down.	See the procedures described in Section 3.2 Worst Case Procedure on page 25.

2.1 Disturbances or Stoppage in Traffic Processing

This section describes the scenario of disturbance or stoppage in traffic processing.

Fact – Platform or Operating System:

Virtual CSCF

Alarm:

See Table 2, Table 3, Table 4

Notification/Event:

Not Applicable



Symptom:	SIP requests are rejected
Symptom:	Diameter requests are rejected
Symptom:	Reduced capacity because of closed port on payloads
Recovery procedures:	See Section 3.1 Disturbances or Stoppage in Traffic Processing on page 7
Risk:	The traffic handling can, sometimes, get even worse after performing maintenance operations
Duration:	The approximate time to complete this procedure is two hours
Expected outcome:	Traffic processing capacity is fully restored

2.2 Worst Case Scenario

This section describes the worst case scenario, that is, if the CSCF system is down.

Fact – Platform or Operating System:	Virtual CSCF
Fact:	All applicable recovery procedures exhausted
Fact:	No further emergency recovery procedures applicable
Recovery procedure:	Section 3.2 Worst Case Procedure on page 25
Magnitude:	This recovery procedure has been calculated as taking up to three hours to perform, assuming all required tools and items to perform the procedure are available.
Expected outcome:	CSCF system is back in service



3 Recovery Procedures

The procedures in this section describe the various scenarios used to find and resolve faults that can cause a CSCF emergency situation.

Note: Do not perform the following activities at system failure unless otherwise stated.

The following activities can be used to find and resolve faults that can cause emergency situations:

- Alter user databases.
- Modify anything other than configuration. Before modifying the configuration, always make a backup copy of the original configuration file.
- Introduce any additional changes (deltas).
- Power off or reboot.
- Change the network level.
- Change any system passwords.

The philosophy of recovery procedures is as follows:

- Identify the problem type best matching the problem experienced.
- Identify the recovery scenario best matching the problem experienced.
- Execute recovery actions in increasing order of severity.
- If the recovery is successful, take preventive actions to prevent problem from reoccurring.

3.1 Disturbances or Stoppage in Traffic Processing

The execution of the procedures follows the workflow as shown in Figure 1:

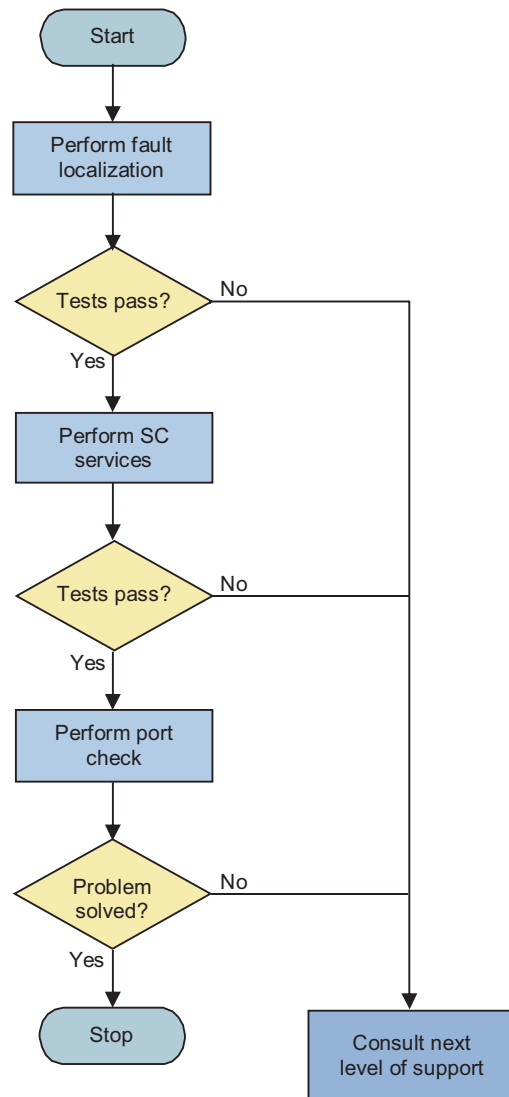


Figure 1 Workflow – Disturbances or Stoppage in Traffic Processing

The following tools are needed for these procedures:

- NBI for Alarm and Notification
- CSCF Health Check
- Ericsson Command-Line Interface (ECLI) and NETCONF

3.1.1 Localize the Fault

Figure 2 shows how to localize the fault, and the detailed descriptions are listed in Table 2.

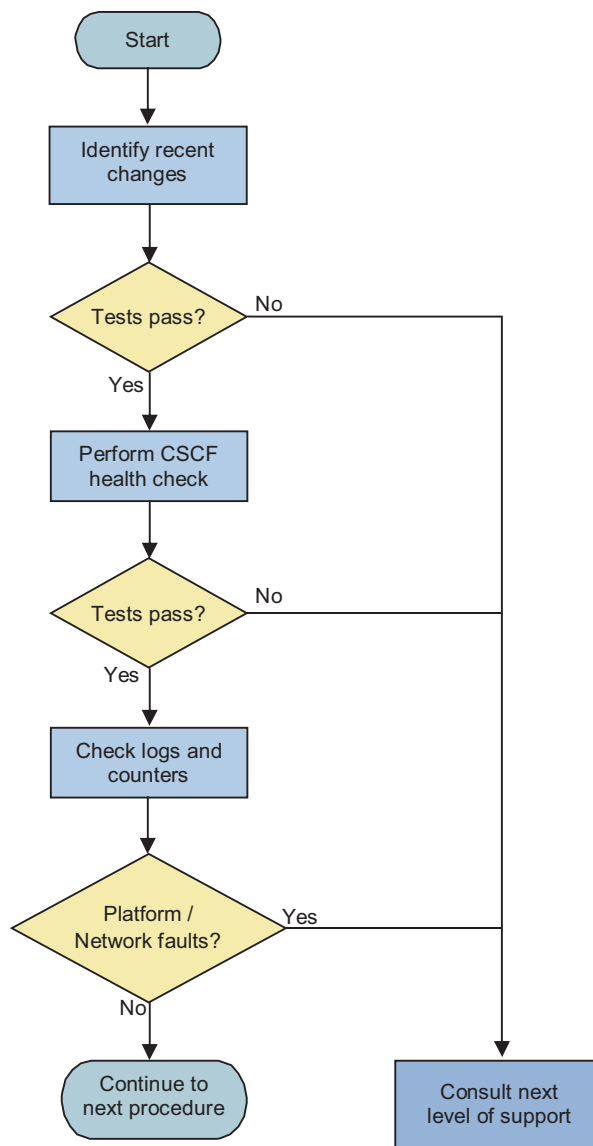


Figure 2 Workflow – Localize the Fault

Table 2 Descriptions of Fault Localization Scenarios

Scenarios	Description
Symptoms	<ul style="list-style-type: none"> SIP request is not forwarded by the CSCF. CSCF responds to all SIP requests with unexpected negative responses.
Severity	<ul style="list-style-type: none"> Major Critical



Scenarios	Description
Possible related alarms	<ul style="list-style-type: none">• Emergency Call Session Control Function (E-CSCF) Receives No LRF Response• Interrogating Call Session Control Function (I-CSCF) LDAP Server Communication Failure• CSCF Throttling of Diameter on Cx/Dx Interface Initiated (threshold alarm)• CSCF Application Locked For Maintenance• CSCF Application Shutting Down• CSCF Degraded Home Subscriber Server (HSS) Redundancy
Description of individual steps	See Figure 2 for the order of steps to be done.

Note: If there is a certain outstanding alarm, follow the documented procedure for troubleshooting that alarm first, except for doing a CSCF or platform reload. Refer to the Customer Product Information (CPI) library for the correct alarm procedure.

3.1.1.1 Identify Recent Changes

To identify recent changes:

1. If the problem started in connection to an update or upgrade, roll back to the last working release, that is, the one not causing any problems.
2. Find out what procedures were performed before the failure, what Correction Packages (CPs) or Emergency Packages (EPs) were added, what files were modified, and so on. If the problem started just after, consider performing a rollback to the last state known to be error free.
3. Identify the type of sessions that are affected. This helps to narrow the scope for troubleshooting. For example, if there are no calls getting through, then problem solving is global, and all aspects of the CSCF, HSS, DNS, Application Server (AS), and Session Border Controller (SBC) connections must be investigated. In this way, the scope of the problem solving is greatly reduced.

Some of the possible session types (not all session types are applicable on all systems) are as follows:

- Register
- Invite



— Subscribe

3.1.1.2 Perform CSCF Health Check

Check the system health, refer to [CSCF Health Check](#). The health check can be run using automatic script `CscfHealthCheck`.

Active alarms are reported in the health check. If any unexpected alarms are found, follow the instructions in the relevant alarm Operating Instruction (OPI) to solve the problem causing the alarm.

3.1.1.3 Check Logs and Counters

To check the logs:

1. Check the contents of the following CSCF applog and console log files:

```
/cluster/storage/no-backup/coremw/var/log/saflog/CSCF*
```

```
/cluster/storage/no-backup/cdclsv/log
```

If there are any CSCF capsule abortions, logs are created in the following folder:

```
/cluster/storage/no-backup/cdclsv/dumps/
```

Specific error or fault messages reported in each log file help to narrow the scope of the problem.

2. Check for platform-related faults in the following folder:

```
/var/log/<node_id>/messages
```

If there are any system core dumps, logs are created in `/cluster/dumps`.

3. Check counter values in the Performance Management (PM) counter reports. If the value of certain counter is abnormal, it could be related to the fault.

The counters are by default generated and (temporarily) stored in directory `/cluster/storage/no-backup/com-apr9010443/PerformanceManagementReportFiles`

For more information about the PM parameters, refer to [Managed Object Model \(MOM\)](#).

Note: The PM counters are automatically transferred to a support system, for example, the Operation and Support System Radio and Core (OSS-RC), so it can be necessary to consult the reports generated by the support system.



If PM counter reports are not generated, it is possible that the PM counters have been disabled or not configured. Contact the next level of support for proper PM configuration.

If there are abnormal numbers of log files, this can indicate a problem with transferring the reports to the Support System. Contact the next level of support for further troubleshooting.

3.1.1.4 Decide If Platform or Network Fault

Based on the information collected in Section 3.1.1.1 Identify Recent Changes on page 10 through Section 3.1.1.3 Check Logs and Counters on page 11, a conclusion can be drawn to decide if the fault is related to platform or network.

To find out if the fault is platform or network-related:

1. Platform issues are raised by the associated alarms and logs. For example, when an individual payload failing to come up on, check for cyclic rebooting in the system log. Contact next level of support to troubleshoot any platform issues.
2. Similarly, network errors can be identified by the associated alarms and logs. For example, an Evolved Virtual IP (eVIP) alarm together with SIP request time-outs are good indications of a network fault.
3. Following the relevant alarm OPIs for any active alarms, identify, and resolve the fault in the network. Keep in mind that local configuration errors can cause some network alarms.

Note: The ways of resolving network faults are outside of the scope of this document.

4. Check if the network has grown and there is a need for proper scaling. The network growth could be caused by the addition of more subscribers or the introduction of new applications. Indications of growth include (but are not limited to) an increase in the average CPU use and increases in counters.

3.1.2 Perform SC Services

The execution of the procedures follows the workflow as shown in Figure 3, and the descriptions of possible scenarios are described in Table 3.

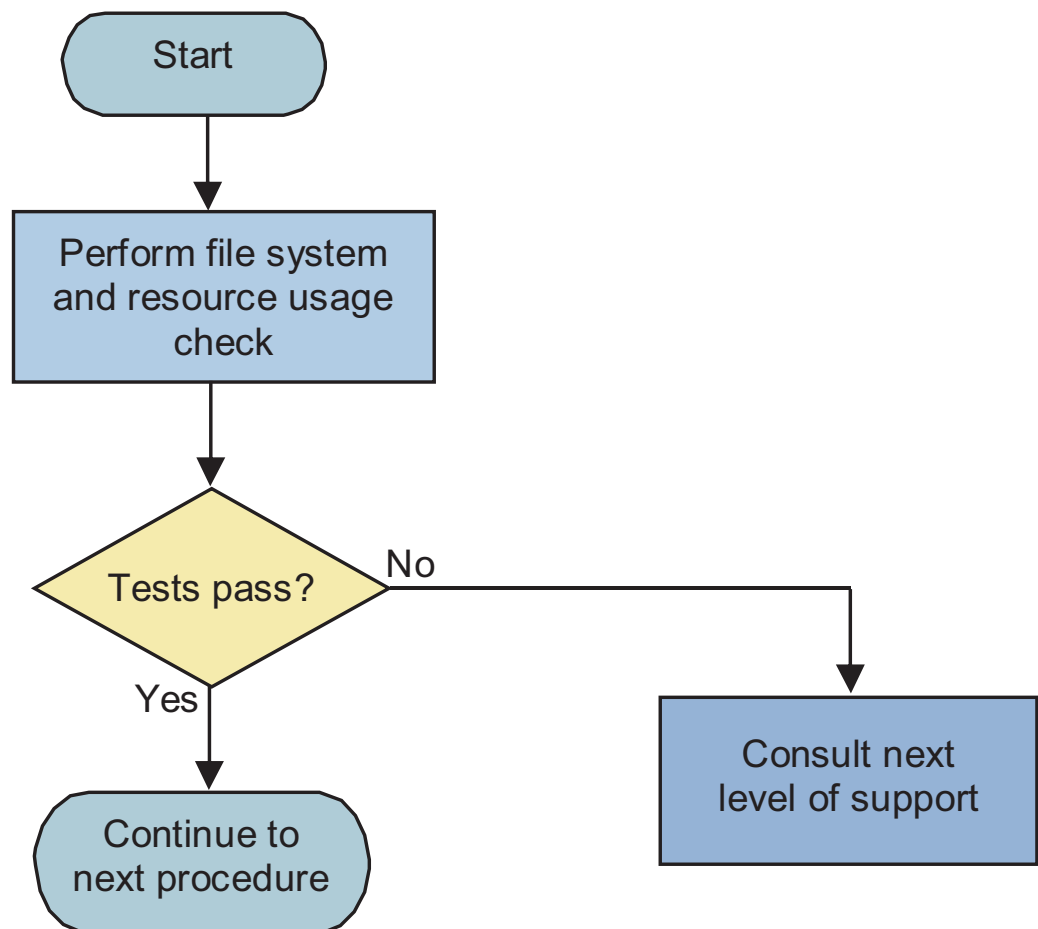


Figure 3 Workflow – Perform System Controller Services

Table 3 Descriptions of System Controller Service Scenarios

Scenario	Description
Symptoms	<ul style="list-style-type: none"> • Problems with charging backups. • BRM backup failures.
Severity	<ul style="list-style-type: none"> • Major • Critical
Possible related alarms	<ul style="list-style-type: none"> • CSCF Charging Backup File System Unavailable • BRM Scheduled Backup Failed
Description of individual steps	See Figure 3 for the order of steps to be done.

Note: If there is a certain outstanding alarm, follow the instructions in the relevant alarm OPI to troubleshoot the alarm first. Refer to the CPI library for the correct the alarm procedure.



3.1.2.1 Check File System and Resource Use

To check the file system and the resource use:

1. Log on to a System Controller (SC):

```
ssh root@<platform_vip_address>
```

2. Show the disk space use of the file system on the SC:

```
df -h
```

If any partition is more than 90% full, clean up the unnecessary files, such as old CA dump and backup files.

3. Show the CPU use:

```
top
```

If a process uses all the CPU, verify which process it is.

4. Log on to the other SC:

```
ssh SC-<x>
```

5. Repeat Step 2 through Step 3 on the other SC.

6. Does the system have a File System (FS) Virtual Machine?

Yes: continue with the next step.

No: proceed with Step 11.

7. Log on to the FS Virtual Machine:

```
ssh <fs-virtual_machine-name>
```

8. Show the disk space on the FS Virtual Machine:

```
df -h
```

If the File Server disk is full, this indicates a problem with offline charging.

9. Show the CPU use on the FS Virtual Machine:

```
top
```

If a process uses all the CPU, verify which process it is.

10. Log off from the FS Virtual Machine:

```
exit
```

11. Verify that the payload CPU and memory uses are normal.



- a. The average CPU and memory use on each traffic payload have been checked by running the `CscfHealthCheck` script in Section 3.1.1.2 Perform CSCF Health Check on page 11.

Example outputs are as follows:

```
CSCF Memory Usage
PL-5:Memory Usage Short Term: 70.8%
                    Long Term: 70.8%
PL-6:Memory Usage Short Term: 70.4%
                    Long Term: 70.4%
PL-7:Memory Usage Short Term: 70.8%
                    Long Term: 70.8%
PL-8:Memory Usage Short Term: 70.8%
                    Long Term: 70.8%
Verdict: OK
...
CSCF CPU Load
PL-5: CPU Load Short Term: 43%
                Long Term: 42%
PL-6: CPU Load Short Term: 40%
                Long Term: 40%
PL-7: CPU Load Short Term: 42%
                Long Term: 42%
PL-8: CPU Load Short Term: 41%
                Long Term: 41%
Verdict: OK
```

- b. Show the CPU use on the Virtual Machine (VM) level:

`clurun.sh cpustat`

An example of printout is as follows:



```
Result from [PL-5.lpmsv.agent.system]:
system command [mpstat -P ALL 1 1 | grep Average] result:
Average: CPU      %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest   %idle
Average: all  31.54    0.11   15.85    0.00    0.00    2.05    0.00    0.00   50.44
Average:   0   38.00    0.00   14.00    0.00    0.00    0.00    0.00    0.00   48.00
Average:   1   36.63    0.00   14.85    0.00    0.00    0.00    0.00    0.00   48.51
Average:   2   22.22    0.00   24.24    0.00    0.00    0.00    0.00    0.00   53.54
Average:   3   27.08    0.00   15.62    0.00    0.00    0.00    0.00    0.00   57.29
Average:   4   33.33    0.00   13.13    0.00    0.00    0.00    0.00    0.00   53.54
Average:   5   31.31    0.00   16.16    0.00    0.00    0.00    0.00    0.00   52.53
Average:   6   39.18    0.00   12.37    0.00    0.00    0.00    0.00    0.00   48.45
Average:   7   30.77    0.00   17.58    0.00    0.00    0.00    0.00    0.00   51.65
Average:   8   32.63    0.00   15.79    0.00    0.00    0.00    0.00    0.00   51.58
Average:   9   34.38    1.04   12.50    0.00    0.00    0.00    0.00    0.00   52.08
Average:  10   34.00    0.00   16.00    0.00    0.00    0.00    0.00    0.00   50.00
Average:  11   29.70    0.00   17.82    0.00    0.00    0.00    0.00    0.00   52.48
Average:  12   30.69    0.00   12.87    0.00    0.00    0.00    0.00    0.00   56.44
Average:  13   34.02    0.00   14.43    0.00    0.00    0.00    0.00    0.00   51.55
Average:  14   36.73    0.00   14.29    0.00    0.00    0.00    0.00    0.00   48.98
Average:  15   26.81    0.00   23.91    0.00    0.00    0.00    0.00    0.00   49.28
Average:  16   16.16    1.01   16.16    0.00    0.00   37.37    0.00    0.00   29.29
Average:  17   36.08    0.00   10.31    0.00    0.00    0.00    0.00    0.00   53.61
```

- c. Show `loadreg` stats to see if traffic is being rejected because of load regulation:

```
clurun.sh printloadreg
```

The output shows the stats per VM, as shown in the following example:

```
Result from [PL-5.lpmsv.agent.vm0]:
Limits:
-----
Limit:                               80%
Memory limit:                        100%
Hysteresis level (on/off): 0%/5%
Maint limit:                         40%
Reconfiguration ongoing:             no
TIPC job queue size:                 5000
Basic Interval:                      1000 ms
Short Intervals:                     10
Short Interval:                      100000 usec
Long term samples:                   5
Current values:                      (<short term>/<long term>)
-----
update count:                        17681
VM Load:                             41.0%/41.6%
*Core load:                          48.0%/51.0% (currently used for load regulation)
Rate delta (CPU):                    -377940345
```



```

Reject Rate (CPU):      0.000 (0)
Memory usage:          71.2%/71.2% (16680484864 bytes free of 57831272448
                        total bytes)
Memory usage base:     66.4%
Rate delta (mem):      -923388150
Reject Rate (mem):     0.000 (0)
MMMap pool page usage: 48.2%/48.2% (4089537 pages allocated of 8471377
                        total pages)
MMMap p. page usage base: 4.1%
Rate delta (mmap):     -356444865
Reject Rate (mmap):    0.000 (0)
Incoming TIPC usage:   0.0%/0.0% (0 jobs allocated of 5000 jobs)
Rate delta (tipc in):  -858967245
Reject Rate (tipc in): 0.000 (0)
Outgoing TIPC usage:   0.0%/0.0% (0 messages allocated of 5000 messages)
Rate delta (tipc out): -858967245
Reject Rate (tipc out): 0.000 (0)
Heap usage:            18.7%/18.6% (268434432 total bytes = 50228208 used
                        bytes + 890464 free bytes)
Heap usage base:       17.0%
Rate delta (heap):     -785961255
Reject Rate (heap):    0.000 (0)
Overall statistics:
-----

```

```

Calls:                1575498
Accepted:              1575498
Rejected all:          0
Rejected CPU:          0
Rejected memory:       0
Rejected MMAP pool:    0
Rejected incoming TIPC: 0
Rejected outgoing TIPC: 0
Rejected heap:         0
Rejected bad priority: 0
Rejected process resource: 0
Per priority statistics:
-----

```

Prio	Incoming	RejCPU	RejMem	RejMMMap	RejTipcIn	RejTipcOut	RejHeap	Rej/Inc	RejRate
0	75	0	0	0	0	0	0	0.000	0.000
1	0	0	0	0	0	0	0	-nan	0.000
2	0	0	0	0	0	0	0	-nan	0.000
3	0	0	0	0	0	0	0	-nan	0.000
4	0	0	0	0	0	0	0	-nan	0.000
5	0	0	0	0	0	0	0	-nan	0.000
6	0	0	0	0	0	0	0	-nan	0.000
7	0	0	0	0	0	0	0	-nan	0.000
8	0	0	0	0	0	0	0	-nan	0.000
9	93	0	0	0	0	0	0	0.000	0.000
10	0	0	0	0	0	0	0	-nan	0.000



11	0	0	0	0	0	0	0	-nan	0.000
12	0	0	0	0	0	0	0	-nan	0.000
13	0	0	0	0	0	0	0	-nan	0.000
14	0	0	0	0	0	0	0	-nan	0.000
15	0	0	0	0	0	0	0	-nan	0.000
16	0	0	0	0	0	0	0	-nan	0.000
17	0	0	0	0	0	0	0	-nan	0.000
18	0	0	0	0	0	0	0	-nan	0.000
19	0	0	0	0	0	0	0	-nan	0.000

The printout changes frequently for short time periods. To have better understanding on how the resources are used on a longer time scale, the command can be executed several times manually or in a script that runs the command many times automatically.

This printout shows how many requests that have been rejected because of CPU or memory or TIPC overload. If abnormal call rejections, contact the next level of support for further troubleshooting.

12. Log off from both SCs:

```
exit
```

3.1.3 Check Closed Ports

This section deals with the scenario where the node has reduced capacity, because of some ports that are stuck in a closed state.

The workflow to resolve reduced capacity because of closed ports is shown in Figure 4, and detailed descriptions are shown in Table 4.

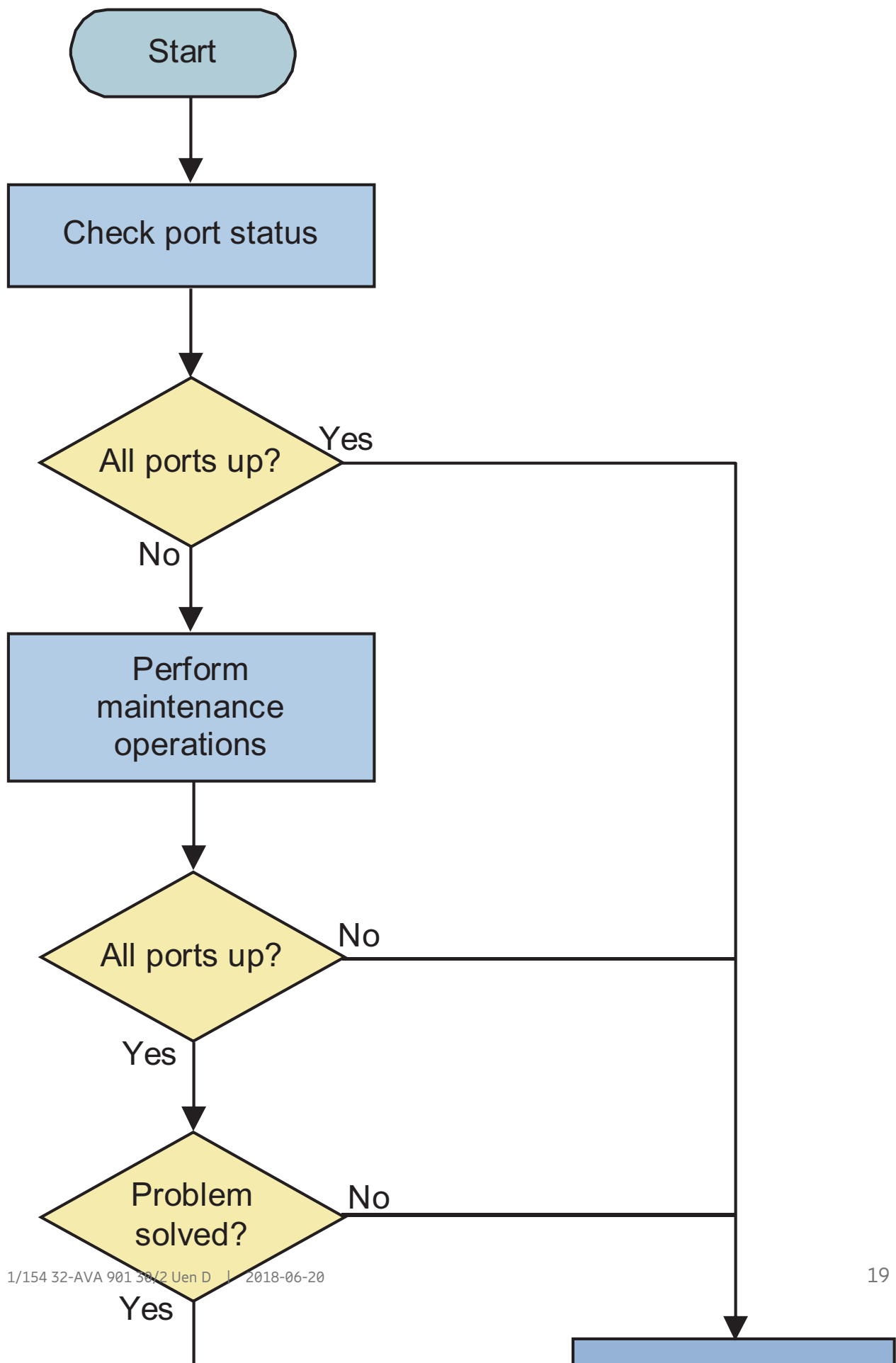




Table 4 Description of Closed Port Scenarios

Scenario	Description
Symptoms	<ul style="list-style-type: none">• ICMP destination unreachable received when sending requests to a specific port.• Diameter link fails to come up.• CSCF SIP Interface Reduced Capacity.• Connection to the NETCONF interface is not possible.
Severity	<ul style="list-style-type: none">• Major• Critical
Possible related alarms	CSCF SIP Interface Reduced Capacity alarm.
Description of individual steps	See Figure 4 for the order of steps to be done.

Note: If there is a certain outstanding alarm, follow the instructions in the relevant alarm OPI to troubleshoot the alarm first. Refer to the CPI library for the correct the alarm procedure.

3.1.3.1

Check Port Status

On each node, there are important ports that must be in LISTEN state. These ports are listed in Table 5.

Table 5 List of Important Ports

Node	Important Ports	Port Name
Serving Call Session Control Function (S-CSCF) interface	5060	SIP port
Proxy Call Session Control Function (P-CSCF) interface	5060, 5062	Gm (5060), Mw (5062)
I-CSCF interface	5060	SIP port
E-CSCF interface	5060	SIP port
Emergency Access Transfer Function (EATF) interface	5060	SIP port
Break-in Control Function (BCF) interface	5060	SIP port



Node	Important Ports	Port Name
Diameter interfaces	3868–3873 or 8700–8738	Diameter ports
Active Common Operation and Maintenance Component (COM) interface	830	NETCONF port
	2022	ECLI port
Operation and Maintenance (O&M)	22	SSH port

SIP and Diameter ports are checked by the `CscfHealthCheck` script, see Section 3.1.1.2 Perform CSCF Health Check on page 11. To verify the port status of these ports, refer to [CSCF Health Check](#).

To check the status of NETCONF, ECLI, and SSH ports:

1. Log on to a System Controller (SC):

```
ssh root@<platform_vip_address>
```

2. Do the following on the SC that runs the active COM:

- a. Check the NETCONF port:

```
for I in SC-1 SC-2; do (echo "---- : $i"; \
ssh $i netstat -ln |grep '830'); done
```

The following is an example output:

```
---- : SC-1
---- : SC-2
tcp      0      0 0.0.0.0:830      0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:830      :::*              LISTEN
```

- b. Check the ECLI port:

```
for I in SC-1 SC-2; do (echo "---- : $i"; \
ssh $i netstat -ln |grep '2022'); done
```

The following is an example output:

```
---- : SC-1
---- : SC-2
tcp      0      0 0.0.0.0:2022     0.0.0.0:*        LISTEN
tcp      0      0 0.0.0.0:2022     :::*              LISTEN
```



Only one SC has port 830 and port 2022 opened, that is because NETCONF and ECLI run on the SC that has the active COM component.

3. Check the SSH port:

a. For the System Controller nodes:

```
for I in SC-1 SC-2; do (echo "---- : $i"; \
ssh $i netstat -ln |grep '22'); done
```

b. For the Payload nodes:

```
for I in $(cdsv-print-node | grep PL | tr '=' ' ' \
|awk '{print $2}' | tr ',' ' '|awk '{print $1}'); \
do (echo "---- : $i"; ssh $i netstat -ln \
|grep '22'); done
```

The following is an example output for the SC nodes:

```
---- : SC-1
tcp      0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp      0      0 0.169.254.100.1:1022 0.0.0.0:*           LISTEN
tcp      0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp      0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
---- : SC-2
tcp      0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp      0      0 0.169.254.100.2:1022 0.0.0.0:*           LISTEN
tcp      0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp      0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
```

4. Log off from the SC:

```
exit
```

3.1.3.2

Perform Maintenance Operations



Attention!

Risk of system malfunction or traffic disturbance.

The procedures in this section have impact on ISP. Get customer approval and contact next level of support before executing the procedures.

At an improper traffic node start, caused by network problems such as an overload, some important ports may not bind properly. In such a situation, a CSCF VM restart or a platform reload can be needed to fix the problem.

The workflow of procedures is shown in Figure 5. The steps are ordered according to their impact severities; proceed with the least impact step first and the most



impact step last. Port status is checked at every step, and the remaining steps can be skipped if all the ports are opened.

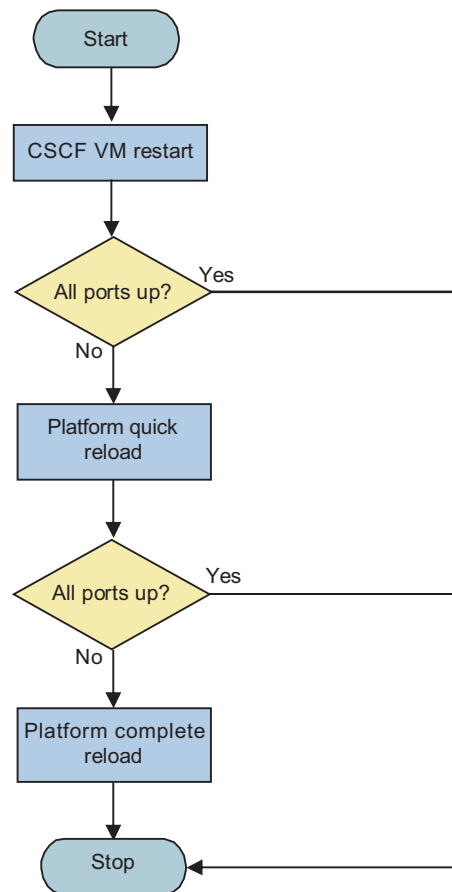


Figure 5 Perform Maintenance Operations

To restart the CSCF VM:

1. Perform a restart to the CSCF VM that has closed ports by the following command.
2. Wait for the restart to finish, and ensure that the restarted CSCF VM has a Started state in the output of the following command:

```
cmw-node-reboot <hostname>
```

```
cdsy-get-node-state
```

If multiple CSCF VMs must be restarted, only perform the restart action on one VM at a time. It causes data loss in the database if a second VM is restarted before the first VM is back in the Started state, and hence trigger a complete platform reload.

Contact next level of support if the CSCF VM is not in the Started state after the restart.



3. See Section 3.1.3.1 Check Port Status on page 20 to recheck the port status. Stop the procedures if all ports are opened.

To perform quick reload of platform:

1. Perform a quick platform reload:

cdsv-cluster-reload CONFIRM

2. Wait for the reload to finish, and ensure that all nodes have a Started state in the output of the following command:

cdsv-get-node-state

Contact next level of support if nodes are not in the Started state after the reload.

3. See Section 3.1.3.1 Check Port Status on page 20 to recheck the port status. Stop the procedures if all ports are opened.

In a quick platform reload, not all platform components are reloaded, so the reload time is relatively short compared to a complete platform reload.

In a complete platform reload, all platform components and the CSCF software are reloaded.

To reload the platform:

1. Check the active backup, the active backup is shown as the Primary Restore Candidate (PRC) in the output of the following command:

lde-brf activelabel -print all -t system

2. If the active backup is the right one, perform a complete platform reload by the following command:

cmw-cluster-reboot and confirm by entering **yes**.

If the active backup is not the right one, perform a system restore to the right backup in ECLI. Refer to [Restore Backup](#).

3. All SSH connections are lost when the system is reloading. After the reload finishes, reconnect to SC:

ssh root@<platform_vip_address>

4. Use the following command to check platform status and ensure that all classes are working OK:

cmw-status app csiass comp node sg si siass su pm

5. Use the following command to check all PLs are in a Started state:

cdsv-get-node-state



6. Contact next level of support if the platform or the CSCF is not in the normal state after the reload.

To recheck the port status, go to Section 3.1.3.1 Check Port Status on page 20.

3.2 Worst Case Procedure

The procedure presented in this section describes the worst case procedure, that is, the CSCF system is down.

The following tools can be needed for this procedure:

- NBI for Alarm and Notification
- UserTrace
- NetTrace
- AppTrace

Note: This instruction refers to procedures in other documents.

To solve the worst case scenario:

1. Contact Ericsson support, see Section 4.2 Consult Next Level of Support on page 27.
2. If requested by Ericsson support, perform a UserTrace / NetTrace / AppTrace capture.

For information on how to use the UserTrace / NetTrace / AppTrace, the different states, levels, and commands, refer to the following documents:

- CSCF User Tracing
- CSCF Network Tracing
- CSCF AppTrace User Guide

3. If requested by Ericsson support, perform a system backup and a system restore to a previous working backup.

Information about how to perform system backup and restore, refer to the following documents:

- Create Backup
- Restore Backup

4. Close Ericsson support; follow up with Customer Service Request (CSR) process, as described in Section 4 on page 27.





4 Report Problems

In general, all described recovery situations must be seen as abnormal and must be reported to the next level of support or according to other documented procedure, log book, and the like, even if the recovery has been successful. Often a CSR is written to a responsible support organization.

If the situation has affected the ISP, it must be reported as such according to documented procedure.

In many situations, it is required to perform a Root Cause Analysis (RCA) afterward to determine the source of the problem. It is therefore important to document carefully the problematic situation and all the recovery steps that have been taken.

Many log files in the system must be saved or copied to another place to prevent them from being overwritten with newer information. It is important that these logs are available for any future RCA.

4.1 Problem Solved

The recovery seems to have worked. Keep the site and the affected functions under extra observation for a while to ensure that the fault does not reoccur.

Record the incident according to local procedures using a log book or similar.

Create a CSR to the next level of support to have the root cause investigated.

4.2 Consult Next Level of Support

Provide the receiving support organization with the following information:

- Site name
- Location
- Operator
- Contact information
- CSCF version loaded, including patches
- Platform version loaded on the node, including patches
- Platform configuration and environment variables setting
- Hypervisor and hardware information
- CSCF configuration



- Problem description
- Procedures followed, including document number
- Information about activities done before, during, and after the incident
- Logs