

vCSCF Network Impact Report from 1.7.0 to 1.8.2

Call Session Control Function

NETWORK IMPACT REPORT

Copyright

© Ericsson AB 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
2	General Impact	3
2.1	Backward Compatibility	3
2.2	Capacity and Performance	3
2.3	Hardware and Platform	3
2.4	Upgrade Impact	3
2.5	Deprecated Features	3
2.6	Obsolete Features	3
2.7	Other Network Elements	3
3	Interfaces	5
3.1	Inter-Node Interface	5
3.2	Operation and Maintenance	5
4	Summary of Impacts per Feature	15
5	Impact on CSCF Features	17
5.1	Emergency Call Handling	17
5.2	Graceful Shutdown	17
5.3	OAM Management (Virtualized)	17
5.4	SIP Request Handling	18
5.5	Traceability and Troubleshooting	19
5.6	Transit Support	19
5.7	VNF Scaling	20





1 Introduction

This Network Impact Report (NIR) describes how the Virtual Call Session Control Function (vCSCF) 1.8.2 with new and enhanced commercial features affects the vCSCF 1.7.0. The NIR also describes the impact on the overall network, including all affected products and functions.

In this document, the term “vCSCF” refers to the product and the term “CSCF” refers to the CSCF application, independent of being deployed in a native or virtual environment.

Note: The vCSCF product is a software-only product. It is not bundled with any hardware platform or virtualization software.

This document covers the following enhanced features:

- Emergency Call Handling
- Graceful Shutdown
- OAM Management (virtualized)
- SIP Request Handling
- Traceability and Troubleshooting
- Transit Support
- VNF Scaling





2 General Impact

This section describes the general impact owing to the introduction of the vCSCF 1.8.2.

2.1 Backward Compatibility

The vCSCF is backward compatible.

2.2 Capacity and Performance

The subscriber capacity increases by the introduction of the vCSCF 1.8.2 if the same version of cloud environment is used.

The performance improves by the introduction of the vCSCF 1.8.2.

2.3 Hardware and Platform

The vCSCF is a software-only product.

The demands on the hardware and platform are specified in [Virtual CSCF Infrastructure Requirements](#).

2.4 Upgrade Impact

Smooth upgrade is supported for the vCSCF 1.7.0 – vCSCF 1.8.2 upgrade.

2.5 Deprecated Features

There are no deprecated features.

2.6 Obsolete Features

There are no obsolete features.

2.7 Other Network Elements

The Northbound Interface (NBI) is modified, which may affect external management systems, for example the Operation and Support System Radio and Core (OSS-RC).





3 Interfaces

This section describes interface changes between the existing and new revisions of the product. The changes to interfaces described here can require changes to the operator systems, technical plans, training of operator personnel, and so on.

No impact indicates that no changes are needed.

3.1 Inter-Node Interface

There are no changed inter-node interfaces.

3.2 Operation and Maintenance

This section describes changes to attributes, alarms, and counters.

3.2.1 Provisioning and Configuration

This section lists changed, deleted, and new attributes.

Further information on attributes can be found in the following documents:

- Managed Object Model (MOM)
- CSCF Configuration Management

3.2.1.1 Changed Attributes

The changed attributes are described in Table 1.

Table 1 Changed Attributes

Attribute Name	Description In vCSCF 1.7.0	Description In vCSCF 1.8.2
OAM Management (virtualized)		



Table 1 Changed Attributes

Attribute Name	Description In vCSCF 1.7.0	Description In vCSCF 1.8.2
cscfAdministrativeState	<p>This attribute indicates the current administrative state of the CSCF. This attribute is used to set the node state to 0 (Locked), 1 (Unlocked), or 2 (Shutting down).</p> <p>A short description of the behavior of CSCF at different states of cscfAdministrativeState is given here.</p> <p>When the node is in state: 0 (Locked), the CSCF is to be taken out of service as soon as possible. Established sessions, except emergency sessions, are released, users are deregistered, and new SIP requests are rejected.</p> <p>When the node is in state: 1 (Unlocked), the CSCF node handles requests and performs functions normally.</p> <p>When the node is in state: 2 (Shutting down), the CSCF is gracefully taken out of service with minimal traffic disturbance. As long as users are registered, non-register traffic is processed as when in Unlocked state. Users are de-registered/re-distributed when handling registration traffic. When all users are de-registered/re-distributed and all sessions are terminated, the CSCF automatically transits from Shutting down to Locked state.</p> <p>The default value is 0 (Locked).</p>	<p>This attribute indicates the current administrative state of the CSCF. This attribute is used to set the node state to 0 (Locked), 1 (Unlocked), or 2 (Shutting down).</p> <p>A short description of the behavior of the CSCF at different states of cscfAdministrativeState is given here.</p> <p>When the node is in state: 0 (Locked), the CSCF is to be taken out of service as soon as possible. cscfAdministrativeState is not allowed to change from Locked to Unlocked when cscfLockedbehavioris FORCED and still in active state. It is also not allowed to change cscfAdministrativeState from Locked to Shutting down.</p> <p>When the node is in state: 1 (Unlocked), the CSCF node handles requests and performs functions normally.</p> <p>When the node is in state: 2 (Shutting down), the CSCF is gracefully taken out of service with minimal traffic disturbance and the CSCF automatically transits from Shutting down to Locked or Unlocked, depending on the configuration.</p> <p>The default value is 0 (Locked).</p>
Transit Support		



Table 1 Changed Attributes

Attribute Name	Description In vCSCF 1.7.0	Description In vCSCF 1.8.2
extNetSelPoolMode	<p>This attribute defines if the pool is considered to be in allocated number mode.</p> <ul style="list-style-type: none"> Prerequisite for changing extNetSelPoolMode to 0 is a configured extNetSelPoolURI. Prerequisite for changing extNetSelPoolMode to 1 is a configured ExtNetSelUnallocatedNrResponseCode. <p>When changing pool mode, all data in the pool that is not used in the new pool mode is automatically erased.</p> <p>Possible Values and Meanings:</p> <ul style="list-style-type: none"> 0 – allocated number 1 – unallocated number 	<p>This attribute defines the result type of the External Network Selection analysis.</p> <ul style="list-style-type: none"> Prerequisite for setting extNetSelPoolMode to ALLOCATED_NUMBER is a configured ExtNetSelPoolURI. Prerequisite for setting extNetSelPoolMode to UNALLOCATED_NUMBER is a configured ExtNetSelUnallocatedNrResponseCode. No prerequisite for setting extNetSelPoolMode to TRANSIT or NON_TRANSIT. <p>When changing pool mode, all data in the pool that is not used in the new pool mode automatically is erased.</p> <p>Possible Values and Meanings:</p> <ul style="list-style-type: none"> 0: ALLOCATED_NUMBER - means that the received SIP request is routed. 1: UNALLOCATED_NUMBER - means that the received SIP request is rejected. 2: TRANSIT - means that the received request is identified to be a transit call. 3: NON_TRANSIT - means that HSS is queried before routing the SIP request.
tcscfBehavior	<p>This attribute controls if HSS (LIR) Lookup(s) are performed or not, on the terminating side of I-CSCF.</p> <p>The attribute cscfISPBehavior must be configured to 1 (standalone I-CSCF) when tcscfBehavior is enabled. This attribute is preparing to introduce a new Transit Function CSCF (also referred to T-CSCF).</p> <p>Possible Values and Meanings:</p> <ul style="list-style-type: none"> 0: DISABLED - HSS (LIR) lookups are performed in the I-CSCF for terminating traffic. 1: ENABLED - HSS (LIR) lookups are NOT performed in the I-CSCF for terminating traffic. 	<p>This attribute controls if HSS (LIR) lookups are performed, not performed, or transit verification is done on the terminating side of the I-CSCF.</p> <p>The attribute cscfISPBehavior must be configured to 1 (standalone I-CSCF) when tcscfBehavior is ENABLED.</p> <p>Possible Values and Meanings:</p> <ul style="list-style-type: none"> 0: DISABLED - HSS (LIR) lookups are performed in the I-CSCF for terminating traffic. 1: ENABLED - HSS (LIR) lookups are NOT performed in the I-CSCF for terminating traffic. 2: TRANSIT_VERIFICATION - transit verification is done before HSS (LIR) lookups in the I-CSCF for terminating traffic to avoid HSS lookups.



Table 1 Changed Attributes

Attribute Name	Description In vCSCF 1.7.0	Description In vCSCF 1.8.2
VNF Scaling		
cscfProcessBehaviourAtClusterReconfiguration	<p>This parameter is used to indicate the CSCF process termination behavior during Cluster Reconfiguration.</p> <p>Cluster Reconfiguration occurs during:</p> <ul style="list-style-type: none">• CSCF software upgrade• CSCF Cluster Instance Lock (Virtual deployment locking of VM instance)• CSCF Scale-In and Scale-Out (Virtual deployment only) <p>Possible Values and Meanings:</p> <ul style="list-style-type: none">• IMMEDIATE = The CSCF application processes are terminated directly. This behavior is preferable for CSCF software upgrade as it reduces the upgrade time. A SIP session that has not been established when reconfiguration happens, fails since the CSCF loses all SIP state information because of the terminated processes. <p>The default value is IMMEDIATE.</p>	<p>This parameter is used to indicate the CSCF process termination behavior during Cluster Reconfiguration.</p> <p>Cluster Reconfiguration occurs during:</p> <ul style="list-style-type: none">• CSCF software upgrade• CSCF Cluster Instance Lock (Virtual deployment locking of VM instance)• CSCF Scale-In and Scale-Out (Virtual deployment only) <p>Possible Values and Meanings:</p> <ul style="list-style-type: none">• DELAYED = The CSCF application processes get some extra time, up to 55 seconds, to be terminated gracefully.• IMMEDIATE = The CSCF application processes are terminated directly. A SIP session that has not been established when reconfiguration occurs, fails since the CSCF loses all SIP state information because of the terminated processes. <p>The default value is DELAYED.</p>

3.2.1.2 Deleted Attributes

There are no deleted attributes.

3.2.1.3 Deprecated Attributes

There are no deprecated attributes.

3.2.1.4 Obsolete Attributes

There are no obsolete attributes.

3.2.1.5 New Attributes and Environment Variables

The new attributes are described in Table 2.

Table 2 New Attributes

Attribute Name	Description
OAM Management (Virtualized)	



Table 2 New Attributes

Attribute Name	Description
cscfLockedBehavior	<p>This attribute describes the behavior of the CSCF during the Locked state. The configured value takes effect when <code>cscfAdministrativeState</code> is set to 0 (LOCKED). This attribute is not access-aware.</p> <p>Possible values are GRACEFUL, IGNORE_REQUESTS, and FORCED.</p> <p>The default value is GRACEFUL.</p>
SIP Request Handling	
cscfBlacklistingThresholdInterval	<p>This attribute defines the measurement period, in seconds, for blacklisting thresholds.</p> <p>This attribute applies to the following SIP blacklisting reasons:</p> <ul style="list-style-type: none"> • SIP 503 Response with Retry-After • SIP 503 Response without Retry-After • SIP transaction time-out • Fatal transport error (socket error) <p>Accepted range: 0 – 86400</p> <p>When it is set to 0, only <code>CscfDestinationUnavailabilityTimer</code> (or the Retry-After header for SIP 503 responses with Retry-After) is used as measurement period for blacklisting thresholds and blacklisting period.</p>



Table 2 New Attributes

Attribute Name	Description
cscfBlacklistingThresholdIntervalDest	<p>This attribute defines the measurement period, in seconds, for blacklisting thresholds for specific destinations in the network.</p> <p>This attribute applies to the following SIP blacklisting reasons:</p> <ul style="list-style-type: none">• SIP 503 Response with Retry-After• SIP 503 Response without Retry-After• SIP transaction time-out• Fatal transport error (socket error) <p>Possible values: default or [0–9]{1,10}</p> <p>Accepted length: 1–7</p> <p>When it is set to default, there is no specific configuration for the destination.</p>
Transit Support	
extNetSelectionInitialTransitTableName	<p>This parameter must be configured with the name of the ENS table to indicate where to start a navigating table for transit verification. The referenced table must be configured before this parameter can be changed.</p> <p>A defined ENS navigation and matching for transit verification. For example: SipMessage:[tableName], calling:[tableName], P-Asserted-Identity:[tableName], CIC:[tableName], RN:[tableName] or called:[tableName].</p> <p>Default value: None.</p>

There are no new environment variables.

3.2.2 Fault Management

This section describes alarms that have been changed, deleted, or added.

3.2.2.1 Changed Alarms

The new alarms are described in Table 3.



Table 3 Changed Alarms

Alarm Name	Description of Change
Transit Support	
CSCF External Network Selection Initial Table Incorrectly Configured	<p>The alarm also is raised when the <code>extNetSelectionInitialTransitTableName</code> parameter is set to an empty table that does not contain any entries, or when some other configuration error is discovered in the ENS tables.</p> <p>For the initial table <code>extNetSelectionInitialTableName</code>, the Additional Text field states Configured Initial Table <table type>:<tablename> is empty.</p> <p>For the initial transit table <code>extNetSelectionInitialTransitTableName</code>, the Additional Text field states Configured Initial Transit Table <table type>:<tablename> is empty.</p>
CSCF External Network Selection Memory Limit Reached	When this alarm is raised, any transit verification causes all SIP messages to be handled as non-transit.
CSCF External Network Selection Table Loop Detected	<p>This alarm indicates if a loop was detected in the transit verification analysis or in the External Network Selection analysis.</p> <p>The Additional Info field is extended as <code>R:SipMessage=[INVITE tel:+468000000000 SIP/2], SdpMediaType=[]</code> or <code>T:SipMessage=[INVITE tel:+468000000000 SIP/2], SdpMediaType=[]</code>, where R stands for External Network Selection and T stands for transit verification.</p>

3.2.2.2 Deleted Alarms

There are no deleted alarms.

3.2.2.3 Deprecated Alarms

There are no deprecated alarms.

3.2.2.4 Obsolete Alarms

There are no obsolete alarms.



3.2.2.5 New Alarms

There are no new alarms.

3.2.3 Events and Notifications

This section describes events and notifications that have been changed, deleted, or added.

3.2.3.1 Changed Events and Notifications

There are no changed events and notifications.

3.2.3.2 Deleted Events and Notifications

There are no deleted events and notifications.

3.2.3.3 Deprecated Events and Notifications

There are no deprecated events and notifications.

3.2.3.4 Obsolete Events and Notifications

There are no obsolete events and notifications.

3.2.3.5 New Events and Notifications

There are no new events and notifications.

3.2.4 Counters

This section describes counters that have been changed, deleted, or added.

3.2.4.1 Changed Counters

There are no changed counters.

3.2.4.2 Deleted Counters

There are no deleted counters.

3.2.4.3 Deprecated Counters

There are no deprecated counters.



3.2.4.4 Obsolete Counters

There are no obsolete counters.

3.2.4.5 New Counters

There are no new counters.





4 Summary of Impacts per Feature

This section summarizes the impact per feature when the feature is turned off, as listed in Table 4.

The description of impact is as follows:

- **Major Impact** means that the feature has done an incompatible change so that another node requires an update.
- **Minor Impact** means that the feature has caused changes that affect other nodes, but with extra configuration, the previous behavior can be kept.
- **No Impact** means that the feature has no impact on the system.

Table 4 Impacts per Feature

Feature	Impact			Basic or Optional New or Enhanced	Included in Value Packs	Relation to Other Features or Nodes
	Major	Minor	No			
Emergency Call Handling			X	Optional Enhanced	Voice. Service Identity SIP Trunking Dynamic User	
Graceful Shutdown			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	HSS
OAM Management (virtualized)			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	
SIP Request Handling			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	SIP Nodes



Table 4 Impacts per Feature

Traceability and Troubleshooting			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	Core Networks Operations Manager
Transit Support			X	Optional Enhanced	Transit	
VNF Scaling		X		Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	



5 Impact on CSCF Features

This section shows the impact on the CSCF features when the feature is turned on.

5.1 Emergency Call Handling

This section describes the enhanced feature Emergency Call Handling.

5.1.1 Description

If an emergency call is rejected by the last Public Safety Answering Point (PSAP) assigned by the Location Repository Function (LRF), and the default PSAP is not configured or the call is a service test call, the Emergency Call Session Control Function (E-CSCF) forwards the SIP error response that it received from the last failed PSAP to the caller. This behavior applies to an E-CSCF with a SIP-based MI interface.

5.2 Graceful Shutdown

This section describes the enhanced feature Graceful Shutdown.

5.2.1 Description

To get a faster graceful shutdown behavior and not prevent the Serving Call Session Control Function (S-CSCF) to automatically transit from Shutting Down to Locked state, a new behavior for the unregistered users is introduced.

When `cscfAdministrativeState` is set to **SHUTTINGDOWN**, unregistered users are started to be deregistered by the S-CSCF. Any new session establishment attempt related to services for unregistered or not-registered users are rejected through a SIP 480 response when `scscfRedundantScscfEntry` is empty. When `scscfRedundantScscfEntry` is configured, they are rejected through a SIP 305 response.

When all registered users are deregistered, the S-CSCF automatically sets `cscfAdministrativeState` to **LOCKED**, even when any unregistered users remain in the S-CSCF.

5.3 OAM Management (Virtualized)

This section describes the enhanced feature OAM Management (Virtualized).



5.3.1 Description

When the CSCF is in the Administrative State Locked, the new parameter `cscfLockedBehavior` defines the behavior of the CSCF.

The parameter `cscfLockedBehavior` has the following settings:

— GRACEFUL

When `cscfAdministrativeState` is set to **0** (LOCKED), the Serving Call Session Control Function (S-CSCF) responds with a 480 (Temporarily Unavailable) response for initial registration, re-registration, and registration of a new contact. All other SIP requests are rejected by 503 (Service Unavailable) responses that are enhanced with the value 5 mins (300 sec) in the Retry-After header. This triggers the client nodes to redirect or blacklist the CSCF in the state LOCKED, so it disconnects all sessions and deregisters all users. The updated 503 (Service Unavailable) response message is applicable for all other CSCF node types.

— IGNORE_REQUESTS

When `cscfAdministrativeState` is set to **0** (LOCKED), the S-CSCF does not respond to any incoming initial SIP requests; it does not send 480 (Temporarily Unavailable) to REGISTER requests or 503 (Service Unavailable) to other requests. The S-CSCF still sends BYE messages to terminate all sessions, SAR, 3rd party REGISTER, and NOTIFY requests to de-REGISTER all users.

All other CSCF node types ignore the incoming initial SIP requests when `cscfAdministrativeState` is set to **0** (LOCKED).

— FORCED

When `cscfAdministrativeState` is set to **0** (LOCKED), all CSCF nodes immediately close the SIP ports. This means that all external signalling stops. The S-CSCF silently terminates all sessions and removes all registered and unregistered users.

5.4 SIP Request Handling

This section describes the enhanced feature SIP Request Handling.

5.4.1 Description

It is possible to configure the time period for accumulating the blacklisting thresholds interval separately from the blacklisting duration period. The threshold interval can be configured per Fully Qualified Domain Name (FQDN), next to the global configuration.



It applies to the following SIP blacklisting reasons:

- SIP 503 with Retry-After header
- SIP 503 without Retry-After header
- Transaction time-out
- Fatal transport error

If the threshold for one of these reasons is exceeded during the measurement period, the blacklisting period starts. During the blacklisting period, received requests are not forwarded to the blacklisted destination.

5.5 Traceability and Troubleshooting

This section describes the enhanced feature Traceability and Troubleshooting.

5.5.1 Description

The CSF is enhanced to align the CSF Health Check output format structure and use with other IP Multimedia Subsystem (IMS) Virtual Network Functions (VNFs). The new XML[®] output format enables using the results in a networking monitoring tool. The CSF also supports new command line options for the Health Check script.

5.6 Transit Support

This section describes the enhanced feature Transit Support.

5.6.1 Description

The transit function in a terminating Interrogating Call Session Control Function (I-CSF) is enhanced with a transit verification function that enables determination if SIP requests must be transited based on configurable criteria. All SIP requests that fulfill the configured criteria are handled as transit requests for which Home Subscriber Server (HSS) queries are suppressed. All SIP requests that do not fulfill the configured criteria are handled as non-transit requests.

For example, when a terminating I-CSF receives a SIP request with a telephone number in its Request-URI, the transit verification function compares the originating network information in the received Via header and the called number in the received Request-URI with the configured criteria. If `extNetSelectionInitialTransitTableName` is not configured or the referenced table is misconfigured, all SIP requests are handled as non-transited requests.

The transit verification function is configurable for a standalone I-CSF and a collocated IS-CSF.



5.7 VNF Scaling

This section describes the enhanced feature VNF Scaling.

5.7.1 Description

The configuration attribute `cscfProcessBehaviourAtClusterReconfiguration` can be set to a new value: **DELAYED**. This new value delays the process termination so the traffic disturbance during Cluster Reconfiguration is reduced.