

vCSCF Network Impact Report from 1.5 to 1.6.0

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	4
3	Interfaces	5
3.1	Inter-Node Interface	5
3.2	Operation and Maintenance	5
4	Summary of Impacts per Feature	11
5	Impact on CSCF Features	13
5.1	Load Regulation	13
5.2	SIP Request Handling	13
5.3	VNF Robustness	14





1 Introduction

This Network Impact Report (NIR) describes how the Virtual Call Session Control Function (vCSCF) 1.6.0 with new and enhanced commercial features affects the vCSCF 1.5. 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:

- Load Regulation
- SIP Request Handling
- VNF Robustness





2 General Impact

This section describes the general impact owing to the introduction of the vCSCF 1.6.0.

2.1 Backward Compatibility

The vCSCF is backward compatible.

2.2 Capacity and Performance

The subscriber capacity is not affected by the introduction of the vCSCF 1.6.0 if the same version of cloud environment is used.

The performance is not affected by the introduction of the vCSCF 1.6.0.

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

The vCSCF 1.5 – vCSCF 1.6.0 upgrade must not be performed with any traffic that is running in the node. It is recommended to migrate the traffic to one or more redundant Serving Call Session Control Function (S-CSCF) nodes and to perform the upgrade with Network Redundancy. For details about the impact, refer to *vCSCF Upgrade Information from 1.5 to 1.6.0*.

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

The changes to the inter-node interfaces are listed in Table 1.

The description of impact is as follows:

- **No Impact** means that the new version can be installed without affecting other nodes.
- **Minor Impact** means that there are changes, but with extra configuration the previous behavior can be kept.
- **Major Impact** implies that the change has made an interface backwards incompatible.
- **New Interface** indicates that the interface did not exist in the previous revision.
- **Obsolete** means that the interface no longer exists.

Table 1 Inter-node Interfaces

Interface	Protocol	Impact	Description of Change Compared to vCSCF 1.5
All Interfaces	All Protocols	No Impact	When eVIP FE-HA is used, the connectivity towards the Cloud Edge switch must use static routing without BFD.

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 2.

Table 2 *Changed Attributes*

Attribute Name	Description in vCSCF 1.5	Description in vCSCF 1.6.0
Load Regulation		
cscfSipOverloadControlReactingTrafficPriorities	<p>This attribute is used to map the outgoing SIP requests to SIP overload control reacting internal priority levels. Two priority levels are supported, where value 0 is the highest one. This attribute is only applicable when <code>cscfSipOverloadControlReactingEnabled</code> is true. This attribute is not access-aware.</p> <p>This attribute can be configured as a string, where the priority is provided first and then a list of SIP request groups. The possible groups are Emergency, RphWps0, RphWps1, RphWps2, RphWps3, RphWps4, Inside, and Default.</p> <p>Default value is 0:Emergency, RphWps0, RphWps1, RphWps2, Inside; 1:Default.</p>	<p>This attribute is used to map the outgoing SIP requests to SIP overload control reacting internal priority levels. 16 priority levels are supported, where value 0 is the highest one. This attribute is only applicable when <code>cscfSipOverloadControlReactingEnabled</code> is true. This attribute is not access-aware.</p> <p>This attribute can be configured as a string, where the priority is provided first and then a list of SIP request groups. The possible groups are Emergency, RphWps0, RphWps1, RphWps2, RphWps3, RphWps4, Inside, and Default.</p> <p>Default value is 0:RphWps0, RphWps1; 1:RphWps2, RphWps3; 2:RphWps4; 3:Emergency; 6:Inside; 15:Default.</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 3.

Table 3 *New Attributes*

Attribute Name	Description
SIP Request Handling	



Table 3 New Attributes

Attribute Name	Description
cscfProactiveMonitoredSipInterfaceEntry	<p>This is the key attribute of the parameter CscfProactiveMonitoredSipInterface. It defines the SIP interface to be monitored. Each entry consists of a CSCF source transport address together with the destination IP address. Both the source and destination address must use the same IP version (IPv4 or IPv6).</p> <p>The value is in the form of: <code><protocol>:<src_address>:<src_port>-<dest_address>[:dest_port]</code>, where:</p> <ul style="list-style-type: none"> • <code>protocol</code>: UDP or TCP. • <code>src_address</code>: an IPv4 dotted decimal address or IPv6 address of the source node. • <code>src_port</code>: the port of the source node, in the range of 1024–49151. • <code>dest_address</code>: an IPv4 dotted decimal address or IPv6 address of the destination node. • <code>dest_port</code>: the destination port. An optional parameter in the range of 1024–49151. If the port is not specified, port 5060 to this destination is used.



Table 3 New Attributes

Attribute Name	Description
cscfProactiveMonitoringInterval	<p>This attribute defines the period in seconds between each SIP OPTIONS used for periodic proactive monitoring.</p> <p>Value 0 means that the periodic proactive monitoring is disabled or discontinued.</p> <p>The default value is 15.</p>
cscfSipMonitoringSuppressDestinationEntry	<p>This attribute defines one or several destination nodes that the CSCF does not monitor by sending SIP OPTIONS when blacklisted. This prevents the blacklisted destinations that do not support SIP OPTIONS, from becoming permanently blacklisted. Monitoring suppression takes effect for both TCP and UDP transport protocols.</p> <p>The value is in the form of: address[:port], where:</p> <ul style="list-style-type: none">• Address: an IPv4 dotted decimal address or an IPv6 address.• Port: an optional parameter in the range of 1024–49151. If the port is not specified, all ports for this destination are suppressed.

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

There are no changed alarms.

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			
Load Regulation			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	SIP nodes supporting the Reporting Role for SIP Overload Control (RFC7339) HSS
SIP Request Handling			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	SIP Nodes
VNF Robustness			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 Load Regulation

This section describes the enhanced feature Load Regulation.

5.1.1 Description

Reacting Role for SIP Overload Control

The CSCF is enhanced to support 16 configurable priority levels, instead of 2, to consider when deciding which requests to redirect or reject: 0 for the highest priority messages, 1–14 for the medium priority messages, and 15 for the lowest priority messages.

During overload, messages with the lowest priority are rejected or redirected randomly first, while high priority messages continue as normal. When the overload is large and cannot be solved through rejecting and redirecting all low priority messages, also messages with the next higher priority are randomly rejected or redirected.

5.2 SIP Request Handling

This section describes the enhanced feature SIP Request Handling.

5.2.1 Description

Suppression of Network Monitoring

When Network Monitoring is enabled by setting `cscfMonitorEnabled` to `true`, the CSCF monitors all unreachable and blacklisted nodes by sending SIP `OPTIONS` to the nodes.

With Network Monitoring for non-compliant nodes, a filter list, defined in `cscfSipMonitoringSuppressDestinationEntry`, can be configured to avoid sending SIP `OPTIONS` to blacklisted nodes that ignore SIP `OPTIONS` to prevent them from being blacklisted permanently. The CSCF supports configuration of a list with up to 100 destination nodes.

Proactive Network Monitoring

A proactive list, defined in `cscfProactiveMonitoredSipInterfaceEntry`, can be configured to monitor sensitive, crucial SIP nodes, and stand-by SIP nodes continuously without considering whether they are blacklisted. The CSCF supports configuration of a list with up to 354 entries. Each entry is configured as a source transport address and a destination address. The source transport address is a configured SIP interface in the CSCF node. The proactive monitoring period is defined in `cscfProactiveMonitoringInterval`.

5.3 VNF Robustness

This section describes the enhanced feature VNF Robustness.

5.3.1 Description

The Evolved Virtual Internet Protocol (eVIP) Front-End High Availability (FE-HA) enables the operator to use a network configuration that does not use Bidirectional Forwarding Detection (BFD) or Open Shortest Path First (OSPF) from the Cloud Edge switch towards the Virtual Network Function (VNF). This limits the requirements that the VNF has on the infrastructure and makes it possible to deploy the VNF when BFD is not supported.

When using eVIP FE-HA, the eVIP Front-End Elements (FEEs) are always available. If one Virtual Machine (VM) that hosts an FEE fails, this Front-End Element is relocated automatically to another VM without an FEE. If no VM without an FEE exists, the Front-End Element is moved to a VM that already hosts an FEE. When the move is complete, it is announced through graceful Address Resolution Protocol (ARP).

The eVIP FE-HA can only be used for configurations with static routing without BFD. Therefore, the Front-End Elements included in an Abstract Load Balancer (ALB) must be reconfigured to use static routing. Also, a first hop redundancy protocol, such as Virtual Router Redundancy Protocol (VRRP), is required in the Cloud Edge switch for redundancy.