

vCSCF Network Impact Report from 1.9.x to 1.11.0

Call Session Control Function

NETWORK IMPACT REPORT

Copyright

© Ericsson AB 2019. 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	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	19
5	Impact on CSCF Features	23
5.1	3rd Party Registration	23
5.2	Authentication	23
5.3	Load Regulation	24
5.4	OAM Management (Virtualized)	24
5.5	Offline Charging	25
5.6	P-CSCF Restoration	25
5.7	SIP Request Handling	25
5.8	Traceability and Troubleshooting	26
5.9	User Initiated Registration/Deregistration	27
5.10	VNF-LCM Workflows	27
5.11	VNF Robustness	28
5.12	VNF Scaling	28





1 Introduction

This Network Impact Report (NIR) describes how the Virtual Call Session Control Function (vCSCF) 1.11.0 with new and enhanced commercial features affects the vCSCF 1.9.x. 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:

- 3rd Party Registration

- Authentication

Note: The enhancements in this feature are valid for all authentication features in the CSCF.

- Load Regulation

- OAM Management (Virtualized)

- Offline Charging

- P-CSCF Restoration

- SIP Request Handling

- Traceability and Troubleshooting

- User Initiated Registration/Deregistration

- VNF-LCM Workflows

- VNF Robustness

- VNF Scaling





2 General Impact

This section describes the general impact because of the introduction of the vCSCF 1.11.0.

2.1 Backward Compatibility

The vCSCF is backward compatible, except for synchronizing Number Normalization configuration.

The configuration of Number Normalization is changed. The same function level exists, but the method for synchronizing the configuration is changed. See Number Normalization Configuration Synchronization in Section 5.4 OAM Management (Virtualized) on page 24.

The previous non-backward compatible EATF changes are removed.

2.2 Capacity and Performance

The subscriber capacity decreases slightly by the introduction of the vCSCF 1.11.0 if the same version of cloud environment is used.

The network performance is not affected by the introduction of the vCSCF 1.11.0.

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

Smooth upgrade is supported for the vCSCF 1.9.x – vCSCF 1.11.0 upgrade.

2.5 Deprecated Features

There are no deprecated features.



2.6 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 backward 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 1.9.x
ISC	SIP	No Impact	Redistribution of application server traffic in CSCF is enhanced by configuration of the parameter <code>scscfReregAsEntry</code> .

3.2 Operation and Maintenance

This section describes changes to attributes, alarms, SNMP alerts, 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 1.9.x	Description In vCSCF 1.11.0
SIP Request Handling		
cscfBlacklistingBypassThrottle	<p>This parameter controls what percentage of initial SIP requests is to be sent to destinations that have been blacklisted as unreachable for other reasons than transaction time-out. It is possible to define the percentage of requests that should be sent in this case.</p> <p>If <code>CscfBlacklistingBypassThrottle</code> has the value 0, it means that CSCF behaves as recommended in standards, that is, send a 500 error if all destinations are blacklisted. How long a destination is blacklisted depends on the reason why it was blacklisted.</p> <p>If <code>CscfBlacklistingBypassThrottle</code> has the value 100, it means that no matter what the reason is, and for how long the node is blacklisted, the CSCF tries to send initial SIP requests towards it in 100% of the cases (that is, ignore the blacklisting completely).</p> <p>If <code>CscfBlacklistingBypassThrottle</code> has another value, for example 70, it means that 70% of all requests disregards the blacklisting and the initial SIP requests are sent anyway.</p>	<p>This parameter controls what percentage of initial SIP requests is to be sent to destinations that have been blacklisted as unreachable because of a SIP 503 with Retry-After. It is possible to define the percentage of requests that should be sent in this case.</p> <p>As long as at least one destination transport address is not blacklisted, that address is used and this parameter has no effect.</p> <p>If <code>cscfBlacklistingBypassThrottle</code> has the value 0, it means that CSCF does not overrule blacklisting for destinations blacklisted because of SIP 503 with Retry-After. The unreachable destination transport address is blacklisted for a configurable period of time (<code>cscfDestinationUnavailabilityTimer</code>).</p> <p>If blacklisting reason is SIP 503 with Retry-After and <code>cscfBlacklistingBypassThrottle</code> has the value 100, it means that no matter for how long the node is blacklisted, the CSCF tries to send initial SIP requests towards it in 100% of the cases: that is, ignore the blacklisting completely.</p> <p>If <code>cscfBlacklistingBypassThrottle</code> has another value, for example 70, it means that 70% of all requests disregards the blacklisting and the initial SIP requests are sent anyway.</p>



Table 2 Changed Attributes

Attribute Name	Description In vCSCF 1.9.x	Description In vCSCF 1.11.0
cscfBlacklistingInsideDialogRequestBypassThrottle	<p>This parameter controls how much of inside dialogue SIP requests should be sent to destinations that have been blacklisted as unreachable. It is possible to define the percentage of inside dialogue SIP requests that should be sent in this case.</p> <p>If <code>cscfBlacklistingInsideDialogRequestBypassThrottle</code> has the value 0, it means that CSCF behaves as recommended in standards, that is, send a 500 error if all destinations are blacklisted. How long a destination is blacklisted depends on the reason why it was blacklisted.</p> <p>If <code>cscfBlacklistingInsideDialogRequestBypassThrottle</code> has the value 100, it means that no matter what the reason is, and for how long the node is blacklisted, the CSCF tries to send inside dialogue SIP requests towards it in 100% of the cases (that is, ignore the blacklisting completely).</p> <p>If <code>cscfBlacklistingInsideDialogRequestBypassThrottle</code> has another value, for example 70, it means that 70% of all requests disregard the blacklisting and the requests are sent anyway.</p>	<p>This parameter controls how much of inside dialogue SIP requests should be sent to destinations that have been blacklisted as unreachable. It is possible to define the percentage of inside dialogue SIP requests that should be sent in this case. As long as at least one destination transport address is not blacklisted, that address is used and this parameter has no effect.</p> <p>If <code>cscfBlacklistingInsideDialogRequestBypassThrottle</code> has the value 0, it means that CSCF does not overrule blacklisting for any inside dialogue SIP request. How long a destination is blacklisted depends on the reason why it was blacklisted.</p> <p>If <code>cscfBlacklistingInsideDialogRequestBypassThrottle</code> has the value 100, it means that no matter what the reason is, and for how long the node is blacklisted, the CSCF tries to send inside dialogue SIP requests towards it in 100% of the cases (that is, ignore the blacklisting completely).</p> <p>If <code>cscfBlacklistingInsideDialogRequestBypassThrottle</code> has another value, for example 70, it means that 70% of all requests disregard the blacklisting and the requests are sent anyway.</p>



Table 2 Changed Attributes

Attribute Name	Description In vCSCF 1.9.x	Description In vCSCF 1.11.0
cscfBlacklistingSipTransactionTimeoutBypassThrottle	<p>This parameter controls how many initial SIP requests should be sent to destinations that have been blacklisted as unreachable because of a SIP Transaction time-out. It is possible to define the percentage of requests that should be sent in this case.</p> <p>If CscfBlacklistingSipTransactionTimeoutBypassThrottle has the value 0, it means that CSCF behaves as recommended in standards, that is, send a 500 error if all destinations are blacklisted. The unreachable destination transport address is blacklisted for a configurable period of time (CscfDestinationUnavailabilityTimer).</p> <p>If blacklisting reason is SIP Transaction time-out and CscfBlacklistingSipTransactionTimeoutBypassThrottle has the value 100, it means that no matter for how long the node is blacklisted, the CSCF tries to send requests towards it in 100% of the cases (that is, ignore the blacklisting completely).</p> <p>If CscfBlacklistingSipTransactionTimeoutBypassThrottle has another value, for example 70, it means that 70% of all requests disregards the blacklisting and the requests are sent anyway. This parameter takes precedence over CscfBlacklistingBypassThrottle in case blacklisting reason is SIP Transaction time-out.</p> <p>This parameter is a sequence with only one element. To change its value with the ECLI, use one of these syntaxes:</p> <pre>cscfBlacklistingSipTransactionTimeoutBypassThrottle[@1]=<new_value></pre> <pre>cscfBlacklistingSipTransactionTimeoutBypassThrottle[<old_value>]=<new_value></pre>	<p>This parameter controls how many initial SIP requests should be sent to destinations that have been blacklisted as unreachable because of a SIP Transaction time-out. It is possible to define the percentage of requests that should be sent in this case. As long as at least one destination transport address is not blacklisted, that address is used and this parameter has no effect.</p> <p>If cscfBlacklistingSipTransactionTimeoutBypassThrottle has the value 0, it means that CSCF does not overrule blacklisting for destinations blacklisted because of SIP transaction time-out. The unreachable destination transport address is blacklisted for a configurable period of time (cscfDestinationUnavailabilityTimer).</p> <p>If blacklisting reason is SIP Transaction time-out and cscfBlacklistingSipTransactionTimeoutBypassThrottle has the value 100, it means that no matter for how long the node is blacklisted, the CSCF tries to send requests towards it in 100% of the cases (that is, ignore the blacklisting completely).</p> <p>If cscfBlacklistingSipTransactionTimeoutBypassThrottle has another value, for example 70, it means that 70% of all requests disregards the blacklisting and the requests are sent anyway.</p> <p>This parameter is a sequence with only one element. To change its value with the ECLI, use one of these syntaxes:</p> <pre>cscfBlacklistingSipTransactionTimeoutBypassThrottle[@1]=<new_value></pre> <pre>cscfBlacklistingSipTransactionTimeoutBypassThrottle[<old_value>]=<new_value></pre>

3.2.1.2 Deleted Attributes

There are no deleted attributes.

3.2.1.3 Deprecated Attributes

The deprecated attributes are described in Table 3.



Table 3 Deprecated Attributes

Attribute Name	Description
OAM Management (Virtualized)	
numberNormalisationTableSync	This parameter is replaced by numberNormalisationTableEditAction, numberNormalisationTableSyncState, and numberNormalisationTableCommitAction.

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 4.

The new environment variables are described in Table 5.

Table 4 New Attributes

Attribute Name	Description
3rd Party Registration	
scscfReregAsEntry	Each entry in this multi-value attribute holds an IP address of an AS instance. For these IP addresses, CSCF invokes 3rd party registration for re-registration when a 3rd party registration trigger is configured in the service profile of a user even if the Registration Type is not configured with re-registration. An empty list means that the function is disabled. Default value: <No Value>.
OAM Management (Virtualized)	
numberNormalisationTableSyncState	This attribute is read-only. It indicates the state of Number Normalization table by changing its value among Initial, Editing, Syncing and Active. The default value is Initial.
numberNormalisationTableEditAction	This attribute is run through ECLI for activating editing of Number Normalization table. It does not have a default value.



Table 4 New Attributes

Attribute Name	Description
numberNormalisationTableCommitAction	<p>This attribute is run through ECLI for committing synchronization of Number Normalization table.</p> <p>It does not have a default value.</p>
SIP Request Handling	
cscfBlacklistingSip503WithoutRetryAfterBypassThrottle	<p>This parameter controls how much of initial SIP requests should be sent to destinations that have been blacklisted as unreachable because of a SIP 503 without Retry-After. It is possible to define the percentage of requests that should be sent in this case.</p> <p>As long as at least one destination transport address is not blacklisted, that address is used and this parameter has no effect.</p> <p>If cscfBlacklistingSip503WithoutRetryAfterBypassThrottle has the value 0, it means that CSCF does not overrule blacklisting for destinations blacklisted because of SIP 503 without Retry-After. The unreachable destination transport address is blacklisted for a configurable period of time (cscfDestinationUnavailabilityTimer).</p> <p>If blacklisting reason is SIP 503 without Retry-After and cscfBlacklistingSip503WithoutRetryAfterBypassThrottle has the value 100, it means that no matter for how long the node is blacklisted, the CSCF tries to send requests towards it in 100% of the cases (that is, ignore the blacklisting completely).</p> <p>If cscfBlacklistingSip503WithoutRetryAfterBypassThrottle has another value, for example 70, it means that 70% of all requests disregards the blacklisting and the requests are sent anyway.</p>



Table 4 New Attributes

Attribute Name	Description
cscfBlacklistingTransportErrorBypassThrottle	<p>This parameter controls how much of initial SIP requests should be sent to destinations that have been blacklisted as unreachable because of a Fatal Transport Error or an ICMP Error. It is possible to define the percentage of requests that should be sent in this case.</p> <p>As long as at least one destination transport address is not blacklisted, that address is used and this parameter has no effect.</p> <p>If <code>cscfBlacklistingTransportErrorBypassThrottle</code> has the value 0, it means that CSCF does not overrule blacklisting to destinations blacklisted because of Fatal Transport Error or ICMP Error. The unreachable destination transport address is blacklisted for a configurable period of time (<code>cscfDestinationUnavailabilityTimer</code>).</p> <p>If blacklisting reason is Fatal Transport Error or ICMP Error and <code>cscfBlacklistingTransportErrorBypassThrottle</code> has the value 100, it means that no matter for how long the node is blacklisted, the CSCF tries to send requests towards it in 100% of the cases (that is, ignore the blacklisting completely).</p> <p>If <code>cscfBlacklistingTransportErrorBypassThrottle</code> has another value, for example 70, it means that 70% of all requests disregards the blacklisting and the requests are sent anyway.</p>
cscfTcpConfigurationId	<p>This is the key attribute of the <code>cscfTcpConfiguration</code> containing configurable TCP attributes for SIP interfaces. One instance of the <code>cscfTcpConfiguration</code> with the key <code>cscfTcpConfigurationId=0</code> is created at startup. It is impossible to create instances. This instance cannot be deleted.</p>



Table 4 New Attributes

Attribute Name	Description
cscfTcpRetransmissionTimeout	<p>This attribute is used to configure the time in seconds that transmitted data can remain unacknowledged before the TCP forces the corresponding connection to close. A value of 0 means that the TCP uses the system default settings. A change of this attribute can take up to 5 minutes to take effect and only affects new TCP connections.</p> <p>Possible values: 0–1200.</p> <p>The default value is 0.</p>
cscfTcpSessionConnectTimeout	<p>This attribute is used to configure the maximum time in seconds that SYN retransmits are sent before aborting the attempt to establish a connection. A change of this attribute can take up to 5 minutes to take effect and only affects new TCP connections.</p> <p>Possible values: 1, 3, 7, 15, 31, and 63.</p> <p>The default value is 31.</p>
cscfTcpSessionDelayAck	<p>This attribute is used to configure TCP optimization for reducing the number of ACKs required to acknowledge outstanding segments. A change of this attribute can take up to 5 minutes to take effect.</p> <p>Possible values and meaning:</p> <ul style="list-style-type: none">• default: Leave the decision to enter or leave quick ACK-mode to TCP.• enabled: Turn on TCP optimization for reducing the number of ACKs that is required to acknowledge outstanding segments.• disabled: Turn off TCP optimization for reducing the number of ACKs that is required to acknowledge outstanding segments. <p>The default value is default.</p>



Table 4 New Attributes

Attribute Name	Description
cscfTcpSessionInactiveTimeout	<p>This attribute is used to configure the time in seconds the connection needs to remain idle before closing the connection. It is recommended to set the value of this attribute to a value larger than that of cscfMonitorFallbackCheckTimer. The change of this attribute can take up to 5 minutes to take effect and only affects new TCP connections.</p> <p>Possible values: 1–3600.</p> <p>The default value is 60.</p>
cscfTcpSessionNoDelay	<p>This attribute is used to control the Nagle algorithm in TCP, which means if data is buffered until there is enough to send out or not. The change of this attribute can take up to 5 minutes to take effect and only affects new TCP connections.</p> <p>Possible values and meaning:</p> <ul style="list-style-type: none"> • 0: Enable the Nagle algorithm in TCP. • 1: Disable the Nagle algorithm in TCP. <p>The default value is 1.</p>
cscfTcpSessionQueueSize	<p>This attribute is used to configure the maximum number of SIP messages that can queue in a TCP session when SIP messages are sent. If the queue is full, negative responses are returned with relevant socket error information. The change of this attribute can take up to 5 minutes to take effect and only effects new TCP connections.</p> <p>Possible values: 5–100.</p> <p>The default value is 10.</p>
VNF Scaling	
cscfScalingId	<p>This is the key attribute of the CscfScalingClass containing all the scaling-related parameters. One instance of the CscfScalingClass with the key cscfScalingId=default is created at startup. This instance cannot be deleted.</p>



Table 4 New Attributes

Attribute Name	Description
cscfScaleIn	This parameter defines the time and targeted cluster size after scale-in (number of PLs). The default value is N/A.
cscfScaleOut	This parameter defines the time and targeted cluster size after scale-out (number of PLs). The default value is N/A.
cscfTimeBasedScalingEnabled	This parameter is used to enable the time-based scaling alert to trigger the scaling workflow. The default value is false .

Table 5 New Environment Variables

New Environment Variable	Description
Offline Charging	
CSCF_CHARGING_BACKUP_RETRY_LIMIT	This parameter defines the maximum number of retries to back up an offline charging request. After all retries fail, the charging information is lost. Together with parameter CSCF_CHARGING_BACKUP_RETRY_TIMER_INTERVAL, this parameter defines how long time the charging information is cached in the memory at most, but not more than 10 minutes. The value 0 disables caching of the charging information at backup failure. Range: 0–5 Default value: 3
CSCF_CHARGING_BACKUP_RETRY_TIMER_INTERVAL	This parameter defines the time interval between two retries to back up an offline charging request. Together with parameter CSCF_CHARGING_BACKUP_RETRY_LIMIT, this parameter defines how long time the charging information is cached in the memory at most, but not more than 10 minutes. Unit: s Range: 10–180 Default value: 20



3.2.2 Fault Management

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

3.2.2.1 Changed Alarms

The changed alarms are described in Table 6.

Table 6 Changed Alarms

Alarm Name	Description of Change
Offline Charging	
CSCF Charging Backup File System Unavailable	The value of Additional Text is changed to Backup Write Failure or Backup Disk Full.

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

The new alarms are described in Table 7.

Table 7 New Alarms

Alarm Name	Description
OAM Management (Virtualized)	
C-Diameter, Diameter Measurement Threshold Crossed	This generic C-Diameter threshold-based alarm was raised because at the end of the Granularity Period the measured value for one of the DiameterCC measurement types was higher than the configured threshold.



Table 7 New Alarms

Alarm Name	Description
C-Diameter, Peer Connection Congestion	This generic C-Diameter threshold-based alarm indicates congestion in the Own or in the Peer Diameter Node. The congestion was measured on one of the peer connections, that is, the message amount dropped because the diameter link congestion crossed the threshold defined by the related threshold job level.
C-Diameter, RTT to Remote Node Exceed Limits	This generic C-Diameter threshold-based alarm indicates disturbances in egress request message delivery. That is, the message amount dropped because the time-out crossed the threshold defined by the related threshold job.

3.2.3 SNMP Alerts

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

3.2.3.1 Changed SNMP Alerts

There are no changed events and notifications.

3.2.3.2 Deleted SNMP Alerts

There are no deleted events and notifications.

3.2.3.3 Deprecated SNMP Alerts

There are no deprecated events and notifications.

3.2.3.4 Obsolete SNMP Alerts

There are no obsolete events and notifications.

3.2.3.5 New SNMP Alerts

The new SNMP alerts are described in Table 8.



Table 8 New SNMP Alerts

SNMP Alert Name	Description
VNF Scaling	
CSCF Time-Based Scaling	<p>When <code>cscfScaleIn</code> is expired, the following SNMP alert that includes alert name and the additional text is raised: CSCF Time Based Scaling, CSCF Time Based Scale In: <code><numberOfPayload></code></p> <p>When <code>cscfScaleOut</code> is expired, the following SNMP alert that includes alert name and the additional text is raised: CSCF Time Based Scaling, CSCF Time Based Scale Out: <code><numberOfPayload></code>.</p>

3.2.4 Events and Notifications

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

3.2.4.1 Changed Events and Notifications

There are no changed events and notifications.

3.2.4.2 Deleted Events and Notifications

There are no deleted events and notifications.

3.2.4.3 Deprecated Events and Notifications

There are no deprecated events and notifications.

3.2.4.4 Obsolete Events and Notifications

There are no obsolete events and notifications.

3.2.4.5 New Events and Notifications

There are no new events and notifications.

3.2.5 Counters

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



3.2.5.1 Changed Counters

There are no changed counters.

3.2.5.2 Deleted Counters

There are no deleted counters.

3.2.5.3 Deprecated Counters

The deprecated counters are described in Table 9.

Table 9 Deprecated Counters

Counter Name	Description
OAM Management (Virtualized)	
cscfActiveUsers	The measurement status of the PM counter cscfActiveUsers is set to DEPRECATED.
cscfActiveUsersPerProfile	The measurement status of the PM counter cscfActiveUsersPerProfile is set to DEPRECATED.

3.2.5.4 Obsolete Counters

There are no obsolete counters.

3.2.5.5 New Counters

The new counters are described in Table 10.

Table 10 New Counters

Counter Name	Description
OAM Management (Virtualized)	
DiaNode	This C-Diameter Performance Management group consists of 49 new counters. For more information, see Managed Object Model (MOM) .
DiaPeer	This C-Diameter Performance Management group consists of 49 new counters. For more information, see Managed Object Model (MOM) .
DiaPeerConn	This C-Diameter Performance Management group consists of 49 new counters. For more information, see Managed Object Model (MOM) .



4 Summary of Impacts per Feature

This section summarizes the impact per feature when the feature is turned off, as listed in Table 11.

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 11 Impacts per Feature

Feature	Impact			Basic or Optional New or Enhanced	Included in Value Packs and Basic Packs	Relation to Other Features or Nodes
	Major	Minor	No			
3rd Party Registration			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Dynamic User	AS
Authentication			X	Optional Enhanced	Voice Messaging Service Identity SIP Trunking Dynamic User	
Load Regulation			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	SIP nodes supporting the Reporting Role for SIP Overload Control (RFC 7339)
OAM Management (Virtualized)			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	



Table 11 Impacts per Feature

Offline Charging			X	Basic Enhanced	Voice Messaging Dynamic User SIP Trunking Service Identity	Charging Control Function
P-CSCF Restoration			X	Optional Enhanced	Voice Messaging Service Identity SIP Trunking Dynamic User	
SIP Request Handling		X		Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	SIP Nodes
Traceability and Troubleshooting			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	
User Initiated Registratio n/Deregistration			X	Optional Enhanced	Voice Messaging Service Identity SIP Trunking Dynamic User	
VNF-LCM Workflows			X	Optional Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	ENM



Table 11 Impacts per Feature

VNF Robustness			X	Basic Enhanced	Voice Messaging Service Identity SIP Trunking Transit Dynamic User	
VNF Scaling			X	Optional 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 3rd Party Registration

This section describes the enhanced feature 3rd Party Registration.

5.1.1 Description

This enhancement enables 3rd party registration when an AS needs to redistribute users to another AS instance because of different reasons. In most cases, the 3rd party registration trigger is not configured for re-registration, which prevents traffic from being redistributed in time. This problem is solved by enabling the CM parameter `scscfReregAsEntry`.

Redistribution of AS traffic is only needed when AS caching is used, meaning when the parameter `as-profile` is set to 1 in the service profile of a user.

Each entry in the multi-value attribute `scscfReregAsEntry` holds an IP address of an AS instance. For these IP addresses, CSCF invokes 3rd party registration for re-registration requests when a 3rd party registration trigger is configured in the service profile of a user even if the Registration Type is not configured with re-registration.

An empty `scscfReregAsEntry` list means that this function is disabled.

When the traffic handover to the target AS node reaches the desired level, the `scscfReregAsEntry` for the specific AS is disabled.

5.2 Authentication

This section describes the enhanced feature Authentication. The enhancements in this feature are valid for all authentication features in the CSCF.

5.2.1 Description

The CSCF authentication is updated to follow 3GPP standards.

The S-CSCF does not authenticate REGISTER requests when the integrity-protected parameter in the Authorization header of the REGISTER request is set to **auth-done**. This behavior is valid for initial registration, re-registration, de-registration, and querying registration.



5.3 Load Regulation

This section describes the enhanced feature Load Regulation.

5.3.1 Description

Reporting Role for SIP Overload Control

The propagation delay of reporting the cluster average Resource Utilization Information (RUI) is reduced. The algorithm to calculate the sent oc-value from the RUI according to [RFC 7339](#) has changed slightly. There is no longer a need to set PM_COLLECTOR_FLUSH_PERIOD to 1, but the default value of 5 is used. These changes improve the performance and stability of the SIP Overload Control Reporting Role of the CSCF.

5.4 OAM Management (Virtualized)

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

5.4.1 Description

ECIM for eVIP

eVIP is configured by pushing predefined eVIP configurations to the CSCF with the Parameter Database (PDB) tool.

Number Normalization Configuration Synchronization

Number Normalization configuration is no longer synchronized by setting numberNormalisationTableSync. The configuration modification is initiated by running numberNormalisationTableEditAction for active editing and concluded by running numberNormalisationTableCommitAction for committing the synchronization.

New Diameter Stack

The C-Diameter stack is integrated with the vCSCF and removed from vDicos. It is backward compatible, but there are some additional O&M-related enhancements.

Three new alarms, C-Diameter, Diameter Measurement Threshold Crossed, C-Diameter, Peer Connection Congestion, and C-Diameter, RTT to Remote Node Exceed Limits are added. For more information, see Section 3.2.2.5 New Alarms on page 15.

New Diameter throughput/latency Performance Management counters are introduced, see Section 3.2.5.5 New Counters on page 18.



Log Management Framework

With the introduction of the Log Management (LogM) framework, centralized registered log stream management through the Northbound Interface (NBI) is possible. This includes setting the severity filter, performing a manual export of logs, and configuring automatic streaming of log entries towards a log server.

5.5 Offline Charging

This section describes the enhanced feature Offline Charging.

5.5.1 Description

Backup Handling

The Additional Text of alarm CSCF Charging Backup File System Unavailable is updated to indicate that the alarm occurs when backing up charging requests fail because of disk full or disk writing failure.

When the charging backup file system fails to back up charging requests because of disk full or disk writing failure, the charging requests are cached in the memory for a predefined time. During the predefined time, the system retries to back up charging requests for predefined times. After all retries fail, the charging requests are lost.

5.6 P-CSCF Restoration

This section describes the enhanced feature P-CSCF restoration.

5.6.1 Description

The condition to trigger the P-CSCF restoration procedure in S-CSCF is expanded from only triggering when access types contain the strings 3GPP-GERAN, 3GPP-UTRAN, or 3GPP-E-UTRAN, to also trigger when they contain 3GPP-NR.

5.7 SIP Request Handling

This section describes the enhanced feature SIP Request Handling.



5.7.1 Description

Support for Invalid tel URI Format Headers

The P-Asserted-Identity can be used to determine the identity of the served user in the originating S-CSCF or I-CSCF. When there is no valid tel URI available in the P-Asserted-Identity header, but a valid international telephone number is present as the canonical SIP URI in a P-Asserted-Identity header, the CSCF creates a tel URI from the SIP URI and uses it to identify the served user.

Configurable TCP Parameters for SIP Interfaces

TCP parameters for the SIP interfaces in CSCF are configurable on a node level through ECLI and NETCONF. The following TCP parameters are configurable:

- The maximum time in seconds that SYN retransmits are sent before aborting an attempt to establish a connection.
- The amount of time in seconds a connection needs to remain idle before it is closed.
- TCP optimization for reducing the number of ACKs required to acknowledge outstanding segments.
- Control of the Nagle algorithm in TCP, which means if data is buffered until there is enough to send out or not.
- The amount of time in seconds that transmitted data can remain unacknowledged before the TCP forces the corresponding connection to close.
- Maximum number of SIP messages to queue in a TCP session when SIP messages are sent.

CSCF Blacklisting Bypass Configuration for Transport Errors and 503 without Retry-After Header

This enhancement improves the configuration for blacklisting bypass throttle by adding two parameters: `cscfBlacklistingSip503WithoutRetryAfterBypassThrottle` and `cscfBlacklistingTransportErrorBypassThrottle`. This gives more flexibility and control on the traffic that conditionally bypasses the blacklisting.

The overrule behavior of `cscfBlacklistingBypassThrottle` has changed. This parameter still controls the blacklisting overrule behavior for SIP 503 with Retry-After header, but the new parameters control now the overrule behavior for SIP 503 without Retry-After header, Fatal Transport Error, and ICMP Error.

5.8 Traceability and Troubleshooting

This section describes the enhanced feature Traceability and Troubleshooting.



5.8.1 Description

CSCF Health Check Single Sign-On Support

The vCSCF supports Single Sign-On for the CSCF health check to align with the health check functions of the other IMS nodes to simplify the use of the Core Network Operations Manager (CNOM).

5.9 User Initiated Registration/Deregistration

This section describes the enhanced feature User Initiated Registration/Deregistration.

5.9.1 Description

The S-CSCF stores the content of the PVNI header of a selected contact in the originating SIP INVITE request. Any PVNI content stored in REGISTER of the same contact is overwritten by the S-CSCF. Stored PVNI content is not removed if there is no PVNI header in the incoming INVITE.

5.10 VNF-LCM Workflows

This section describes the enhanced feature VNF-LCM Workflows.

5.10.1 Description

Supported Workflows

Table 12 All Supported Workflows In vCSCF 1.11.0

	Full Stack OR-VNFM-Triggered	Full Stack VNFM-Triggered	Small Stack	Small Stack
	Openstack	Openstack	Openstack	VMware
Instantiate	Supported	Not supported	Supported	Supported
Terminate	Supported	Supported	Supported	Supported
Heal	Not supported	Not supported	Supported	Not supported
Managed Scaling	Not supported	Not supported	Supported	Supported

For vCSCF Workflows, the minimum required version of VNF-LCM is 19.02 (Media version: 4.9.15).

For vCSCF Workflows, the minimum required version of vIMS Common Workflow Bundle is 1.15.2. This is part of the delivered workflow pack.



EM-Driven Instantiation

After a successful instantiation operation from the VNF-LCM finishes successfully, a new Virtual Application belonging to the instantiated VNF is available in the EO too.

Time-Based Scaling

The Managed Scaling workflow can be also triggered for time-based scaling on OpenStack and VMware, see Section 5.12 VNF Scaling on page 28.

5.11 VNF Robustness

This section describes the enhanced feature VNF Robustness.

5.11.1 Description

CSCF-Specific Value of TIPC Timer Attribute

To tolerate temporary disturbances in the underlying cloud network, the value of the LDE TIPC timer attribute `link_tolerance` is increased from 1500ms to 5000ms.

LDE Watchdogd Support

The CSCF now supports the `lde-watchdogd` function that LDE provides as a CBA System Model (CSM) component. The `lde-watchdogd` function provides a configurable watchdog daemon that periodically resets the watchdog timer by writing to `/dev/watchdog`.

The watchdog device can be real hardware, emulated hardware, for example by a Kernel Virtual Machine (KVM) hypervisor, or fully implemented in software as a kernel module.

For a hardware watchdog device, the LDE agent watchdog daemon relies that its driver, the kernel module, is loaded. This is determined by checking for the existence of `/dev/watchdog`. If this file is not there when the LDE agent watchdog service is started, the service attempts to load a software watchdog. This results in `/dev/watchdog` appearing, albeit backed by a software-implemented device.

The watchdog configuration that is used by the LDE watchdogd component is set using the parameters provided in the CSM component configuration file `lde-agents-watchdogd.yaml`.

5.12 VNF Scaling

This section describes the enhanced feature VNF Scaling.



5.12.1 Description

The VNF Scaling feature is enhanced with time-based scaling. Time-based scaling is disabled by default.

When time-based scaling is enabled, the CSCF reads configuration parameters `cscfScaleIn` and `cscfScaleOut`, and starts timers for scale-out and scale-in. The parameters `cscfScaleIn` and `cscfScaleOut` configure a time of day for scaling and the number of VMs to scale.

When either timer expires, the CSCF sends an SNMP alert to the VNF-LCM for scaling operations based on a predefined number of VMs at a predefined time of a day.