

SAPC 1 Network Impact Report

Ericsson Service-Aware Policy Controller

NETWORK IMPACT REPORT

Copyright

© Ericsson España, S.A. 2017, 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 Network Impact Report is not to be used for working with real equipment. It is only meant as an informative document.

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	Other Network Elements	1
2	General Impact	1
2.1	Capacity and Performance	1
2.2	Configuration	4
2.3	Changes in Upgrade Procedure	5
2.4	Upgrade Impact in UDC	6
2.5	BackupFormatter Tool	6
2.6	IP Network Design	6
2.7	Other Impacts	9
3	Impacts on Basic Functions	10
3.1	Event Triggers Selection	10
3.2	Flexible Output Protocol	11
3.3	PCEF Restart and PCEF Removal	11
3.4	Policy Studio Improvements in SAPC 1.0	12
3.5	Diameter Race Conditions and Concurrent Reauthorizations over Gx	12
3.6	Performance Data Collection Support	13
3.7	Virtualization and Cloud Improvements in SAPC 1.0	13
3.8	CNOM Support	14
3.9	NB-IoT RAT-Type Support	14
3.10	Virtualization and Cloud Improvements in SAPC 1.1	15
3.11	Session Release due to Subscription Removal	15
3.12	Policy Studio Improvements in SAPC 1.1	16
3.13	Extended QCI Support	17
3.14	Session Cleanup Mechanism Due to Inactivity	17
3.15	UE Trace Tool	18
3.16	Flexible ARP Mapping	18
3.17	CNOM Support Improvements in SAPC 1.1.1	19
3.18	UE Trace Improvements in SAPC 1.1.1	19
3.19	Security Management Improvements in SAPC 1.1.1	20
3.20	Policy Studio Improvements in SAPC 1.1.1	20



3.21	Virtualization and Cloud Improvements in SAPC 1.1.1	20
4	Impacts on Optional Functions	21
4.1	Presence Reporting Area	21
4.2	Emergency Services	22
4.3	External Database Redundancy Support (1+1+1)	23
4.4	Mobility Based Policy Control for Overlay Deployments	24
4.5	AF Restart	25
4.6	Overload Protection of Priority Services	26
4.7	IMS Restoration	27
4.8	Network Location Information for Untrusted WLAN	28
4.9	Notification of Signalling Path Status	29
4.10	Geographical Redundancy Active-Active	30
4.11	IP-CAN Type Change Notification	31
4.12	Usage Limits Aggregation	31
4.13	Delay PCC Rules Installation for Preliminary Service Information	32



1 Introduction

This Network Impact Report (NIR) describes the new and changed functions implemented in the SAPC since SAPC 17A FD01 and indicates how these changes affect the product and the overall network used by operators.

To find the changes applicable to a specific upgrade path, apply the filters by using the funnel icon on the upper left part of the browser.

1.1 Other Network Elements

For information on SAPC compatibility with other Ericsson products, refer to [Compatible Network Elements](#).

2 General Impact

This section provides information about changes in the system that affect general areas.

2.1 Capacity and Performance

This section summarizes the performance of the SAPC in a standalone configuration, using internal repository, in the following network environments:

- **Scenario A**, where the SAPC uses Gx Rel 9 interface towards GGSN. Default Bearer QoS Control is activated.
- **Scenario B1**, where the SAPC uses Ericsson Gx+ Rel 9 interface towards GGSN. Default Bearer QoS Control and Usage Reporting for Mobile functions are activated.
- **Scenario F**, LTE/EPC solution, where the SAPC uses Gx Rel 9 interface towards Ericsson EPG or with any PDN Gateway.
- **Scenario F1**, IMS VoLTE solution

Performance data in this document are based on the Default Traffic Models.

The frequency of the messages received by the SAPC using the Default Traffic Model is as follows:



Scenario A

- 0.238 Default IPCAN bearer activations per subscriber during the Busy Hour.
- 0.238 Default IPCAN bearer deactivations per subscriber during the Busy Hour.
- 1 Gx Interim per session.
- 0.35 sessions per subscriber

Scenario B1

- 0.238 Default IPCAN bearer activations per subscriber during the Busy Hour.
- 0.238 Default IPCAN bearer deactivations per subscriber during the Busy Hour.
- 1 Gx interim per session.
- 0.3 Default IPCAN session modifications owing to Usage Reporting for Mobile per session.
- 100% of the subscribers use Usage Reporting for Mobile function.
- 0.35 IPCAN sessions per subscriber.

Scenario F

- 0.14 IPCAN session establishment per subscriber during the Busy Hour.
- 0.126 IPCAN session release per subscriber during the Busy Hour.
- 2.5 IPCAN session interim per IPCAN session during the Busy Hour.
- 0.7 IPCAN sessions per subscriber.

Scenario F1

- 0.14 IPCAN session establishment per subscriber during the Busy Hour.
- 0.126 IPCAN session release per subscriber during the Busy Hour.
- 2.5 IPCAN session interim per IPCAN session during the Busy Hour.
- 0.7 IPCAN sessions per subscriber.
- 1 AF session establishment per subscriber during the Busy Hour.
- 1 AF session modification per subscriber during the Busy Hour.
- 1 AF session release per subscriber during the Busy Hour.



- 100% of the subscribers use VoLTE services.
- The average duration per AF session is 1.5 minutes.

Note: Subscribers is the number of subscribers provisioned in the node.

2.1.1

Subscriber Capacity and Network Performance

The following data are used for the characteristics measurements for each network scenario previously described.

- Subscriber Profile used for SACC scenarios: 14 authorized services in the Gx interface per IPCAN session. The number of services authorized has impact on the performance of the node.

The following tables show the maximum Subscriber Capacity and the maximum Transactions Per Second of SAPC per each network scenario. The number of TPS supported for all releases of the Gx interface when executing similar functions is about the same.

The concept of Transaction in this document means a service request and the corresponding reply. The related capacity term is Transactions Per Second (TPS).

Table 1 Scenario A: Gx, QoS

Scenario A	2 TP	10 TP	20 TP	34 TP
Millions of Subscribers	7.7	56.0	106.5	173.4
Transactions Per Second	1,529	11,118	21,125	34,400
PDP Sessions (thousands)	2,699	19,621	37,279	60,706

Table 2 Scenario B1: Gx, QoS, Usage Reporting

Scenario B1	2 TP	10 TP	20 TP	34 TP
Millions of Subscribers	5.6	41.1	78.2	127.4
Transactions Per Second	1,233	8,968	17,039	27,747
PDP Sessions (thousands)	1,982	14,413	27,385	44,594

Table 3 Scenario F: LTE/EPC Solution

Scenario F	2 TP	10 TP	20 TP	34TP
Millions of Subscribers	9.1	66.3	126.0	205.2



Scenario F	2 TP	10 TP	20 TP	34TP
Transactions Per Second	1,561	11,351	21,566	35,119
Number of Gx sessions (thousands)	6,386	46,434	88,225	143,667

Table 4 Scenario F1: IMS VolTe Solution

Scenario F1	2 TP	10 TP	20 TP	34 TP
Millions of Subscribers	1.0	7.6	14.4	23.5
Transactions Per Second	1,052	7,651	14,538	23,674
Number of Gx sessions (thousands)	733	5,328	10,123	16,484
AF Sessions (thousands)	26	190	361	589

External Database Access

The impact of storing subscriber profiles in an external database is determined by the performance of the external database, the parts of the subscriber profile externally stored and the operator data model. According to estimations, the impact in performance using LDAP interface is as follows:

- 15% reduction in the number of TPS supported, when both subscriber profile and usage accumulators are stored in external database, which needs a write operation to external database.
- 10% reduction in the number of TPS supported, when no accumulators are stored in the external database.

2.2 Configuration

The differences in the **Managed Object Model (MOM)** since the previous release can be found as part of the MOM, see next Figure:



Figure 1 Location of the differences in the MOM

2.3 Changes in Upgrade Procedure

2.3.1 SAPC 1.0

The upgrade procedure has been improved in SAPC 1 providing:

- Automatic update of configuration files
- Automatic update of Diameter dictionary files
- Automatic update of PM (counters and threshold alarms)
- Automatic update of preconfigured entities
- Upgrade traces for troubleshooting purposes
- Upgrade progress in console
- Automatic installation of new SLES Security patches in the host OS in SCs in SAPC PNF (to improve security in the system)

2.3.2 SAPC 1.1

The upgrade procedure has been improved to consider the increase of memory of the PL VMs in SAPC VNF.

There exist upgrade limitations derived from the changes on the IP Network Design. For further details, refer to Section 2.6 on page 6.



2.4 Upgrade Impact in UDC

2.4.1 SAPC 1.0

When the SAPC is deployed as part of the User Data Consolidation (UDC) solution, consider the following impacts:

- Application schema in CUDB:
 - Added `SevTrig`, `SspId`, `SpdnGwName`, and `SpresenceAreaName` attributes in the SAPC object class.
- Application counters in CUDB: no impacts
- Notification files with CUDB: no impacts
- Notifications with the Provisioning Gateway: no impacts
- Validations in Provisioning Gateway: no impacts

2.4.2 SAPC 1.1

No impacts

2.5 BackupFormatter Tool

The `BackupFormatter` tool can be used to export information contained in the backups of the SAPC internal database.

2.6 IP Network Design

2.6.1 SAPC 1.1

2.6.1.1 VNF

The following impacts must be considered for SAPC VNF deployments:

- A new deployment of SAPC without Virtual Routers is provided as the recommended alternative for SAPC1.1 onwards. It has the following characteristics:
 - SCs and PLs are directly connected to the Datacenter Gateways through static routing.
 - As there are no VRs, the so called VIP Networks become the External Networks.



- The mask for Traffic External network is /28 instead of /29 to cope with the IP addresses assigned to the FEEs.
- The number of FEE elements per SC/PL has been reduced from 2 to 1, keeping the FEE High Availability, so, the minimum number of interfaces per VM is 3 (eth1, eth2, and eth3) instead of the previous 4 interfaces. This is the default configuration in SAPC1.1.
- Physical traffic separation is extended and now can be configured for any of the Traffic types (Gx, Rx, Sy, and so on) supported by SAPC.

Advantage of deployment without VRs is that it needs less resources (do not need 4 VMs for the VRs), provides low failover time when a SAPC VM is not available and avoids unnecessary OSPF signaling. Option with using VRs is kept (optionally) for legacy reasons, for SAPC1.0 customers that were already using them, and do not want to change their IP design.

Attention!

There is no upgrade procedure to remove the Virtual Routers from an existing SAPC deployment with Virtual Routers, a new deployment is needed.

- The deployment of SAPC with Virtual Routers is supported for backward compatibility reasons. Several improvements are included in this solution:
 - The number of FEE elements per SC/PL has been reduced from 2 to 1, keeping the FEE High Availability, so, the minimum number of interfaces per VM is 3 (eth1, eth2, and eth3) instead of the previous 4 interfaces. This is the default configuration in SAPC1.1. Previous FEE configuration with 2 FEE elements per VM is supported for backward compatibility reasons.
 - For SAPC deployments with Virtual Routers, one single OAM VIP Network interconnects both SCs and the OAM Virtual Routers. Similarly, one single Traffic VIP Network interconnects the PLs with FEE elements with Traffic Virtual Routers. Previous networks configuration with 2 OAM VIP Networks and 2 Traffic VIP Networks is supported for backward compatibility reasons.
 - Physical traffic separation is extended and now can be configured for any of the Traffic types (Gx, Rx, Sy, and so on) supported by SAPC.
 - When Virtual Routers are not connected to the OSPF network of the customer, the OSPF area 0 is created in a new interlink between both VRs; VRRP address between VRs is only created in this case.
 - The software of the Virtual Routers is updated to include a new version of the VMware Tools.

Attention!

There is no upgrade procedure to apply these improvements, a new deployment is needed.

For further information, refer to the [SAPC Network Description](#) and [SAPC VNF Network Configuration Guide](#).

2.6.1.2

PNF - NSP

The following impacts must be considered for SAPC NSP deployments:

- Additional configuration is provided for resilience in the internal network: a new management interface in the SCs, connected to the second SCX, together with a new cross-link among the 2 SCXs, allows that the solution works fine when a SCX fails. Also the ARP monitoring added to detect connectivity problems. DMX is used as SCXB and HW management software. Also, a collapsed redundant Northbound Interface is included to the configuration. The details of this new configuration are the following:
 - A new cross-link cable is added to interconnect both Ethernet Switch Boards of subrack 0.
 - .1 for SCXB-0-0 (left).
 - .2 for SCXB-0-25 (right).
 - IP addresses used previously for SCs (sapc_internal_sp network) are reassigned in the SCXB for ARP monitoring:
 - .121 for SC-1.
 - .122 for SC-2.
 - IP addresses from the sapc_mgmt_sp network are also assigned to the hypervisors in the new mgmt2 interface:
 - .3 for Host_1.
 - .4 for Host_2.



Attention!

There is no upgrade procedure to apply this new configuration, a new installation is needed.

- Deployment recommended by the SAPC PNF Deployment Instruction is aligned with the common cabling in production environments: PL-7/PL-8 for traffic purposes, PL-3/PL-4 for external Database, PL-5/PL-6 for GeoRed and PL-9/PL-10 for traffic separation.

For further information, please, refer to the SAPC NSP 6.1 Hardware Description and NSP 6.1 Network Configuration Guide.

2.7 Other Impacts

2.7.1 SAPC 1.0

SCTP

SCTP bundling is disabled by default.

Rx Interface

The Rx interface is enhanced to support the Rx-Request-Type AVP in AAR messages from the Application Function (AF).

The following changes are made to support the Rx-Request-Type AVP:

- When an AAR message is received with this AVP, the SAPC answers an AAA message whose Result-Code AVP is:
 - DIAMETER_UNKNOWN_SESSION_ID (5002) if Rx-Request-Type is UPDATE_REQUEST (1) and there is no Rx session
 - DIAMETER_INVALID_AVP_VALUE (5004) if Rx-Request-Type is PCSCF_RESTORATION (2), given that this value is not supported yet

The following counter is added:

- rxAasUnknownSessionId

2.7.2 SAPC 1.1

REST interface



On the REST interface, the integer attribute of content `pccRuleId` is deprecated as of SAPC 1.1 but still enabled to ensure backward compatibility. A new string attribute `pccRuleName` is added as a replacement of `pccRuleId`. From SAPC 1.1 on, `pccRuleName` must be used instead of `pccRuleId`.

New tag

The new `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].selected` policy tag is added in order to know if the reporting group for a specific data plan is in usage.

3 Impacts on Basic Functions

This section describes features, enhancements, and other changes that are introduced with the software upgrade.

3.1 Event Triggers Selection

Introduced in: SAPC 1.0

3.1.1 Description of Impacts

Event Triggers can be set unconditionally at subscriber, subscriber group, or node levels, and also conditionally using policies.

3.1.2 Interface

Event-Triggers can now be included in Gx CCA-Update and RAR messages.

The following changes are done to support Dynamic Event Triggers:

- Added `Event-Trigger` AVP in CCA-Update and RAR messages
- Added `NO_EVENT_TRIGGERS` (14) value in the `Event-Trigger` AVP in CCA-Update and RAR messages.

3.1.3 Operation

The following policy type is added:

- `event-triggers`



3.2 Flexible Output Protocol

Introduced in: SAPC 1.0

3.2.1 Description of Impacts

The Flexible Output Protocol allows transformations of the outgoing Gx protocol messages that do not affect the SAPC logic, but that are complementary to it. The SAPC supports transformation at command level (message) and at service level (Charging-Rule).

3.2.2 Interface

No impact

3.2.3 Operation

New policies added for Flexible Output Protocol.

3.3 PCEF Restart and PCEF Removal

Introduced in: SAPC 1.0

3.3.1 Description of Impacts

Policy and Charging Enforcement Function (PCEF) restart is detected when any CCR-Initial message is received with an *Origin-State-Id* AVP that is different from the *Origin-State-Id* currently stored in the SAPC.

Note: In previous SAPC releases it was detected only if the received *Origin-State-Id* was higher than the stored one.

When a *diameterNode* peer is removed from the configuration data, the SAPC removes all the sessions established by that peer as done during a PCEF restart, but without applying any delay before starting to delete.

3.3.2 Interface

The SAPC does not reject CCR-Is with *DIAMETER_INVALID_AVP_VALUE* (Result-Code value 5004) in case the CCR-I is received with an *Origin-State-Id* lower than the locally stored one. Any different *Origin-State-Id* is considered for PCEF restart detection instead.

3.3.3 Operation

No impact



3.4 Policy Studio Improvements in SAPC 1.0

Introduced in: SAPC 1.0

3.4.1 Description of Impacts

The Policy Studio function supports the view, creation, modification, and deletion of subscriber profiles. It allows to associate profiles, data plans, reporting groups, and so on, with subscribers. It also supports the visualization of usage accumulators.

3.4.2 Interface

No impact

3.4.3 Operation

No impact

3.5 Diameter Race Conditions and Concurrent Reauthorizations over Gx

Introduced in: SAPC 1.0

3.5.1 Description of Impacts

When a race condition is reported by the PCEF, the SAPC is able to reauthorize the session and send reattempting RARs to the PCEF with the latest policy information. The SAPC does not send a new Gx RAR message to the PCEF until the previous Gx RAR is acknowledged for the same Gx session.

3.5.2 Capacity and Performance

Enabling diameter race conditions and concurrent reauthorization handling over Gx can imply a performance drop of up to 8% in TPS for traffic models with high rate of SAPC-initiated reauthorizations (Gx RAR messages), due to, for example, AF events or time of day conditions.

3.5.3 Interface

The following changes are done to support diameter race conditions and concurrent reauthorization handling:

— Added bit value 16 in the Supported-Features AVP



- Added DIAMETER_PENDING_TRANSACTION (4144) value in Experimental-Result-Code AVP in RAA messages
- Added DIAMETER_OUT_OF_SPACE (4002) value in Result-Code AVP in RAA messages

3.5.4 Operation

New counters added: gxRaasPendingTransaction, gxRaasOutOfSpace.

3.6 Performance Data Collection Support

Introduced in: SAPC 1.0

3.6.1 Description of Impacts

The SAPC provides Performance Data Collection (PDC) support to regularly collect performance data and generate output information.

SAPC 1.0 also supports the health check option containing information about general SAPC status (ports, interfaces and capacity licenses).

Refer to [Performance Data Collection](#) for details.

3.6.2 Interface

No impact

3.6.3 Operation

No impact

3.7 Virtualization and Cloud Improvements in SAPC 1.0

Introduced in: SAPC 1.0

3.7.1 Description of Impacts

The SAPC provides support for deployment and scaling from ATLAS.

The SAPC provides support for deployment and manual scaling from VMware vCloud Director.

3.7.2 Interface

No impact



3.7.3 **Operation**

No impact

3.8 CNOM Support

Introduced in: SAPC 1.0

3.8.1 **Description of Impacts**

The Core Network Operations Manager (CNOM) is an Ericsson separate product not directly provided with the SAPC.

The SAPC provides support to integrate the following applications of CNOM:

- Network monitor
- Alarm monitor
- Health check

3.8.2 **Interface**

No impact

3.8.3 **Operation**

No impact

3.9 NB-IoT RAT-Type Support

Introduced in: SAPC 1.0

3.9.1 **Description of Impacts**

The SAPC supports NB-IoT RAT-Type. The SAPC can evaluate policies for the NB-IoT access type.

3.9.2 **Interface**

No impact

3.9.3 **Operation**

Added new value for `AccessData.bearer.accessType` policy tag.



3.10 Virtualization and Cloud Improvements in SAPC 1.1

Introduced in: SAPC 1.1

3.10.1 Description of Impacts

Due to the Virtualization and Cloud improvements, the following functions are supported:

- Additional workflows for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) in CEE deployments with HEAT
- Minimum resources for the SAPC deployment in Cloud has been modified: Minimum memory for PLs is increased from 7GB to 10GB. Upgrade procedure is provided.
- Dynamic MACs are supported for new SAPC deployments in VMware
- ECM workflows are deprecated

3.10.2 Interface

No impact

3.10.3 Operation

No impact

3.11 Session Release due to Subscription Removal

Introduced in: SAPC 1.1

3.11.1 Description of Impacts

If the Subscriber Profile is removed from the Subscription Profile Repository (SPR) (internal or external), the SAPC requests IP-CAN session termination, sending a RAR request to the PCEF.

3.11.2 Capacity and Performance

Additional SAPC processing and network messages are introduced. Instead of sending only one RAR to update the session, a CCR-T and a CCA-T message are added per Gx session.

3.11.3 Interface

No impact



3.11.4 Operation

No impact

3.12 Policy Studio Improvements in SAPC 1.1

Introduced in: SAPC 1.1

3.12.1 Description of Impacts

Due to the Policy Studio enhancement, the following functions are supported:

- Configuration guide section
- "Read Only" user role
- Presence Reporting Area (PRA) function
- Mobility-Based Policy Control for Overlay Deployments (PDN-GW selection, SPID selection and Smp session control) function
- Multiple notifications at Rule level
- Default SMS destination attribute at dataplan level
- Dataplan description attribute
- Event Triggers management
- Emergency services support
- NB-IoT RAT-Type value
- The `resourceType` attribute is added on content-qos profile level (MCPTT QCI)

3.12.2 Interface

No impact

3.12.3 Operation

- The Policy Studio server listening port is made configurable. The previous port numbers (8585 for HTTP and 8686 for HTTPS) are the default values, but can be changed using the `PORT` configuration variable in the `server.config.json` file.
- The installation and upgrade processes do not require internet access.



3.12.4 Other Impacts

User experience is improved as follows:

- Error situation management is enhanced

3.13 Extended QCI Support

Introduced in: SAPC 1.1

3.13.1 Description of Impacts

The SAPC provides support for the QoS Class Identifiers (QCI) defined for Mission Critical Push-To-Talk (MCPTT) and Vehicle-to-Everything (V2X) services.

The SAPC supports operator-specific QCI values in the range from 128 to 254 that can be configured as either GBR or non-GBR.

3.13.2 Interface

No impact

3.13.3 Operation

The new `resourceType` optional parameter is added to the content-qos profile to allow the configuration of the QCI values as GBR or non-GBR.

3.14 Session Cleanup Mechanism Due to Inactivity

Introduced in: SAPC 1.1

3.14.1 Description of Impacts

The SAPC provides an automatic cleanup mechanism to remove all the Gx sessions that have been inactive (no request has been received or sent for them in a period of time).

3.14.2 Interface

No impact

3.14.3 Operation

The session inactivity cleanup mechanism generates these new logs daily:

- Start deleting inactive sessions.



- End deleting inactive sessions.

3.15 UE Trace Tool

Introduced in: SAPC 1.1

3.15.1 Description of Impacts

The UE Trace Tool enables the operator to collect incoming and outgoing messages for a set of User Equipments (UEs).

3.15.2 Interface

Using the Gx and Rx interfaces, the SAPC:

- Activates or deactivates incoming and outgoing UE traces for a user indicated by the `subscriberId` AVP
- Shows UE trace sessions that are being traced
- Collects messages filtered for subscriber ID in MSISDN or IMSI format

Note: Using the Rx interface, the SAPC can collect messages filtered for subscriber ID in SIP-URI format as well.

- Generates an xml and a pcap file containing messages from all active UE tracing sessions

3.15.3 Operation

The operator is expected to do all the tracing activities using a CLI command.

3.16 Flexible ARP Mapping

Introduced in: SAPC 1.1

3.16.1 Description of Impacts

The Flexible Allocation Retention Priority (ARP) Mapping function enables the SAPC to assign a certain ARP value to a dynamic service based on the received ARP value.

3.16.2 Interface

No impact



3.16.3 Operation

Added the new `AccessData.requestedQos.priorityLevel` policy tag.

Updated the `AccessData.requestQos.classIdentifier` policy tag.

3.17 CNOM Support Improvements in SAPC 1.1.1

Introduced in: SAPC 1.1.1

3.17.1 Description of Impacts

The SAPC provides support to integrate the following application of CNOM:

— UE Trace

3.17.2 Interface

No impact

3.17.3 Operation

No impact

3.18 UE Trace Improvements in SAPC 1.1.1

Introduced in: SAPC 1.1.1

3.18.1 Description of Impacts

Due to this enhancement, the following functions are supported:

— Scheduling trace sessions

— Seeing a trace in real-time using the UE Trace viewer

3.18.2 Interface

No impact

3.18.3 Operation

To accomplish this enhancement, the operator is expected to do all the tracing activities using a CLI command.



3.19 Security Management Improvements in SAPC 1.1.1

Introduced in: SAPC 1.1.1

3.19.1 Description of Impacts

Due to this improvement, the SAPC provides an automatic procedure either to create a self-signed certificate, to install a self-signed certificate, or both, to be used in a secure communication involving the HTTPS protocol.

For more information, see [Security Management Guide](#).

3.19.2 Interface

No impact

3.19.3 Operation

No impact

3.20 Policy Studio Improvements in SAPC 1.1.1

Introduced in: SAPC 1.1.1

3.20.1 Description of Impacts

The self-signed certificate management is improved providing an automatic way of creating and installing it in the SAPC.

3.20.2 Interface

No impact

3.20.3 Operation

No impact

3.21 Virtualization and Cloud Improvements in SAPC 1.1.1

Introduced in: SAPC 1.1.1

3.21.1 Description of Impacts

The Promiscuous mode and Forget Transmits security policy attributes of VMVware Cloud Infrastructure can be set to "Reject" in the Internal0 network,



as it was done in the other networks of the SAPC. This configuration can be done in existing SAPC deployments upgraded to this release, but, it requires a reboot of the cluster.

Dynamic MACs are supported for Virtual Routers interfaces in new SAPC deployments in CEE.

3.21.2 Interface

Not applicable

3.21.3 Operation

No impact

4 Impacts on Optional Functions

4.1 Presence Reporting Area

Introduced in: SAPC 1.0

4.1.1 Description of Impacts

The Presence Reporting Area (PRA) function enables the SAPC to select an area where presence of the subscriber is reported. Only changes of presence relative to the area (that is, whether the subscriber enters or leaves the PRA) are reported by the PCEF, which produces a decrease in signalling. The SAPC makes policy decisions based on the presence of the subscriber in the area and sends the corresponding enforcement actions to the PCEF.

4.1.2 Capacity and Performance

Impact in the traffic model: additional CCR-U messages to report the PRA.

It may have an impact in the node memory in the case that PRA areas are provisioned massively (per subscriber).

4.1.3 Interface

The following changes are done to support Presence Reporting Area in Gx interface:



- Added bit value 23 in the Supported-Features AVP
- Added the Presence-Reporting-Area-Information AVP in CCR and CCA messages
- Added the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) value in the Event-Trigger AVP in CCR, CCA and RAR messages

4.1.4 Operation

The following policy tags are added:

- `AccessData.subscriber.locationInfo.presenceReportingArea["presenceAreaName"].isInArea`
- `AccessData.host.isPraSupported`

The following policy type is added:

- `presence-reporting-area`

4.2 Emergency Services

Introduced in: SAPC 1.0

4.2.1 Description of Impacts

The Emergency Services functionality introduces support for emergency IP-CAN sessions and IMS emergency calls.

4.2.2 Interface

The following changes are made to support emergency services:

- Gx:
 - Added DIAMETER_ERROR_INITIAL_PARAMETERS (5140) value in the Experimental-Result-Code AVP
- Rx:
 - Added the Service-URN AVP in AAR messages
 - Added UNAUTHORIZED_NON_EMERGENCY_SESSION (5066) value in the Experimental-Result-Code AVP



4.2.3 Operation

The following policy tag is added:

- AfData.serviceUrn

The following log events are added:

- AF Emergency Session established
- AF Emergency Session terminated

The following log file that includes emergency service log events only is added:

- emergencyCalls.log

The following measurements are added:

- afEmergencyActiveSessions
- gxCcasErrorInitialParameters
- gxCcasInitEmergencyFailed
- gxCcasInitEmergencySuccess
- ipCanAuthenticatedEmergencyActiveSessions
- ipCanEmergencyActiveSessionsPerApn
- ipCanUnauthenticatedEmergencyActiveSessions
- ipCanUnknownEmergencyActiveSessions
- rxAasInitEmergencyFailed
- rxAasInitEmergencySuccess
- rxAasUnauthorizedNonEmergency

4.3 External Database Redundancy Support (1+1+1)

Introduced in: SAPC 1.0

4.3.1 Description of Impacts

The SAPC allows to define up to three different points of access towards the External Database, each one towards a different site. Each point of access is identified by a different VIP address.



4.3.2 Interface

No impact

4.3.3 Operation

The following measurements are added:

- IdapSearchRequests
- IdapModifyRequests
- IdapSearchResponsesFailed
- IdapModifyResponsesFailed
- soapExtDbNotificationsReceived
- soapExtDbNotificationResponsesFailed

4.4 Mobility Based Policy Control for Overlay Deployments

Introduced in: SAPC 1.0

4.4.1 Description of Impacts

The Mobility Based Policy Control for Overlay Deployments function introduces a new Smp interface between the SAPC and the SGSN-MME that enables the PDN-GW selection and SPID selection.

4.4.2 Capacity and Performance

Smp is a new interface that requires dimensioning. This feature has no impact in the performance for those scenarios where the Smp interface is not used. The performance of the Smp operations is better than the performance of Gx operations as the functionality provided is lighter.

The impact on the performance of the feature mostly depends on:

- Subscribers that are using the Smp interface.
- Traffic model: the frequencies of some operations can become high depending on especially those related to location change.

4.4.3 Interface

The Smp interface is a new interface between the SGSN-MME and the SAPC to provide Mobility Based Policy Control for Overlay Deployments. For details, refer to [Smp Interface Description](#).



This interface uses a non-standard port by default, different than the rest of the Diameter-based interfaces. For more information, refer to [Security Hardening Guide](#).

4.4.4 Operation

New measurements related to Smp interface are added.

The following policy types are added:

- New policy for PDN-GW selection
- New policy for SPID selection
- New policy for Smp access control

For the details, refer to [Smp Interface Description](#).

The following log events are modified or added:

- Error sending CCA
- Internal Error
- License Error
- Protocol Error

4.5 AF Restart

Introduced in: SAPC 1.0

4.5.1 Description of Impacts

AF restart is detected when any Rx-AAR (initial or update) message is received with an `Origin-State-Id` AVP that is different from the `Origin-State-Id` currently stored in the SAPC. After the restart detection, the SAPC starts identifying all the invalid Rx sessions established from the restarted AF and removing them, without any additional delay.

The SAPC executes massive clean-up with low priority, and provides a mechanism to avoid load peaks due to the massive clean-up, so incoming messages are not affected.

4.5.2 Interface

No impact

4.5.3 Operation

No impact

4.6 Overload Protection of Priority Services

Introduced in: SAPC 1.1

4.6.1 Description of Impacts

In overload situation, the SAPC prioritizes the messages handled with higher priority and rejects messages handled with lower priority securing sustainable acceptable throughput and graceful degradation of the system.

When the SAPC is overloaded, the SAPC:

- Rejects the incoming Diameter messages (Gx, Rx, Smp, Sy/ESy) to reduce its load answering with DIAMETER_TOO_BUSY
- Rejects the incoming SOAP notification messages to reduce its load answering with an HTTP Server Error
- Discards the session reauthorization initiated by the SAPC due to the Time Trigger function
- Rejects the incoming REST API messages to reduce its load answering with an HTTP Service Unavailable Error
- Executes massive clean-up with low priority upon PCEF or an AF restart detection

4.6.2 Interface

- Gx: Added the DIAMETER_TOO_BUSY (3004) value in the Result-Code AVP in CCA-Update and CCA-Termination messages
- Rx: Added the DIAMETER_TOO_BUSY (3004) value in the Result-Code AVP in AAA-Update and STA messages
- Sy/Esy: Added the DIAMETER_TOO_BUSY (3004) value in the Result-Code AVP in SNA messages
- Smp: Added the DIAMETER_TOO_BUSY (3004) value in the Result-Code AVP.
- SOAP Notification: the SAPC rejects the incoming notification request processing and returns an error to the SOAP client if the SAPC is overloaded
- REST API: The SAPC rejects any provisioning request through the REST interface and returns a 503 Service Unavailable HTTP error message if the SAPC is overloaded



4.6.3 Operation

The following measurements are added:

- gxCcasInitEmergencyTooBusy
- gxCcasUpdateEmergencyTooBusy
- gxCcasUpdateTooBusy
- gxCcasTerminateTooBusy
- rxAaasInitEmergencyTooBusy
- rxAaasUpdateEmergencyTooBusy
- rxAaasUpdateTooBusy
- rxStasTooBusy
- sySnasTooBusy
- reauthsOnToDTooBusy
- restProvServiceUnavailable
- soapExtDbNotificationsReceivedTooBusy

Updated the following alarms:

- Policy Control, Number of Gx CCAs Initial Sent Indicating Too Busy Reached
- Policy Control, Number of Sx CCAs Initial Sent Indicating Too Busy Reached

4.7 IMS Restoration

Introduced in: SAPC 1.1

4.7.1 Description of Impacts

The Provisioning of AF Signalling Flow Information is a supported feature, it is part of the IMS Restoration Procedures, specified in 3GPP TS 23.380, to handle a Proxy Call Session Control Function (P-CSCF) service interruption scenario with minimum impact to the service to the end user.

After UE registration to IMS, the AF (P-CSCF) sends information to the SAPC about the AF signalling flows between the UE and the AF. The SAPC installs the corresponding dynamic Policy Charging and Control (PCC) rules (if not installed before) by triggering a RAR message in order to convey the AF address the UE is using to the PCEF. The PCEF monitors all P-CSCF nodes being used by the UEs and if a P-CSCF becomes unresponsive, the PCEF requests all UEs using this P-CSCF to do a new registration against another P-CSCF.



4.7.2 Capacity and Performance

This feature has impacts on memory. If P-CSCF uses the Provisioning of AF Signalling Flows function, an Rx signalling session is created additionally to the associated Rx session created for Voice over LTE (VoLTE) calls.

4.7.3 Interface

— Gx:

- New AF-Signalling-Protocol AVP (AVP code 529) in Gx RAR
- New supported-features ProvAFsignalFlow in Feature-List-ID 1

— Rx:

- New AF-Signalling-Protocol AVP (AVP code 529) in Rx AAR
- New supported-features ProvAFsignalFlow in Feature-List-ID 1

4.7.4 Operation

The following policy tag is added:

— `AfData.media.flowUsage`

4.8 Network Location Information for Untrusted WLAN

Introduced in: SAPC 1.1

4.8.1 Description of Impacts

This function enables the SAPC to report the network provided location for Untrusted WLAN information to the AF during session establishment, modification and termination, and IP-CAN session termination and bearer release.

The network provided WLAN location information includes:

- WLAN location information and location information age
- UE local IP address, User Datagram Protocol (UDP) source port, Transmission Control Protocol (TCP) source port
- UE time zone

4.8.2 Interface

— Gx:



- Added the following AVPs in a Gx CCR message: TWAN-Identifier, UE-Local-IP-Address, TCP-Source-Port, UDP-Source-Port
 - Added support for bit 30 (Netloc-Untrusted-WLAN) in the Supported-Features AVP
- Rx:
- Added the following AVPs in Rx RAR and Rx STA messages: TWAN-Identifier, UE-Local-IP-Address, TCP-Source-Port, UDP-Source-Port
 - Added support for bit 16 (Netloc-Untrusted-WLAN) in the Supported-Features AVP

4.8.3 Operation

The following policy tag is added:

— `AccessData.bearer.isAnTrusted`

4.9 Notification of Signalling Path Status

Introduced in: SAPC 1.1

4.9.1 Description of Impacts

The Notification of Signalling Path Status function enables the SAPC to report the release of signalling path from the PCEF to the AF. The precondition is that the AF subscribes to the notification of signalling path status at AF session establishment.

4.9.2 Capacity and Performance

In general, the AF subscribes to the notification of AF signalling path status in a dedicated Rx diameter session, which is different from the Rx diameter session for VoLTE services. Therefore, the number of active Rx diameter sessions is increased that impacts the dimensioning of the node and the capacity license of dynamic policy control.

4.9.3 Interface

— Rx: Supports the AF_SIGNALLING(2) value in the Flow-Usage AVP

4.9.4 Operation

It is needed to configure the default AF signalling service in the AF signalling path profile. It is possible to configure a different AF signalling service per APN.



The following measurements are added:

- rxAarsAfSignalling
- rxAaasAfSignallingSuccess
- rxStrsAfSignalling
- rxStasAfSignallingSuccess
- rxAsrsAfSignalling
- rxAsasAfSignallingSuccess
- afSignallingActiveSessions

The following policy tag is added:

- `AccessData.subscriber.service["serviceName"].isAfSignallingSubscribed`

4.10 Geographical Redundancy Active-Active

Introduced in: SAPC 1.1

4.10.1 Description of Impacts

Geographical redundancy deployment in active-active mode has been added where both active SAPC nodes are able to handle traffic simultaneously.

4.10.2 Interface

No impact

4.10.3 Operation

A new node state is added in the GeoRedManager MO to indicate the local node status for an active-active geographical redundancy.

For more information on active-active geographical redundancy to standalone and hot standby deployments, see the corresponding operating instructions.

4.10.4 Other Impacts

The Diameter Redirection Agent (DRA) or Diameter clients distribute traffic homogeneously between the two mated pair of SAPC nodes. The distribution must ensure subscriber and session stickiness.



4.11 IP-CAN Type Change Notification

Introduced in: SAPC 1.1

4.11.1 Description of Impacts

IP-CAN Type Change Notification enables the SAPC to report IP-CAN type and Radio Access Technology (RAT) type changes from the access network to the AF. If the AF successfully subscribes to the IP-CAN type change notification, the SAPC provides the change information to the AF when the SAPC gets it from the PCEF.

4.11.2 Capacity and Performance

The AF can subscribe to IP-CAN type change notification as part of the IMS SIP registration or during the IMS SIP call negotiation.

IMS SIP registration has impact on the capacity license of dynamic policy control.

Impact in the traffic model: Increase the frequency of AF and Gx operations.

4.11.3 Interface

— Gx:

- New AN-Trusted AVP (AVP code 1503) in Gx CCR messages
- New IP-CAN-Type (AVP code 1027), RAT-Type (AVP code 1032), AN-Trusted (AVP code 1503) and AN-GW-Address (AVP code 1050) AVPs in Gx RAA messages

— Rx:

- New IP-CAN_CHANGE (6) value in the Specific-Action AVP in Rx AAR messages
- New IP-CAN-Type (AVP code 1027), RAT-Type (AVP code 1032), and AN-Trusted (AVP code 1503) AVPs in Rx AAA and Rx RAR messages. AN-GW-Address (AVP code 1050) is also added to the Rx RAR messages.

4.11.4 Operation

No impact

4.12 Usage Limits Aggregation

Introduced in: SAPC 1.1.1



4.12.1 Description of Impacts

The SAPC supports aggregation of a subscriber's absolute usage limits from different subscriber groups and performs fair usage control for the aggregated limits. The SAPC combines respectively the uplink, downlink, bidirectional volume limits and time limits from aggregable Reporting Groups of the subscriber groups associated with the subscriber.

4.12.2 Interface

- New optional aggregable attribute in usage limits for Reporting Groups for subscriber groups in Provisioning REST API.
- New optional object inside Subscriber Accumulator containing aggregated usage limits.

4.12.3 Operation

To aggregate usage limits, it is needed to set the new aggregable attribute to true for the same Reporting Group of the subscriber groups assigned to the subscriber.

4.13 Delay PCC Rules Installation for Preliminary Service Information

Introduced in: SAPC 1.1.1

4.13.1 Description of Impacts

A new `provision_rules_on_preliminary_info` configuration parameter has been added. It supports the installation of PCC rules for preliminary service information, or delaying the installation until the status of the service information is final.

4.13.2 Interface

No impact

4.13.3 Operation

Added new `AfData.requestType` policy tag.