SAPC 1 Network Impact Report

Ericsson Service-Aware Policy Controller

Network Impact Report

109 48-FGC 101 3390/1-V1 Uen AC

Copyright

© Ericsson España, S.A. 2019-2024. 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

Attention!

The N+1 architecture is a fully restricted feature. All N+1 related content has been included in official documentation in order to maintain a single documentation track. This feature cannot be enabled without approval from Ericsson.

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.

Note: From SAPC 1.11.0 (SAPC 1.10.0 with Limited Availability), the SAPC Policy Control Function (PCF) is introduced. The SAPC PCF, as part of the SAPC, performs policy and charging controls related to 5G subscribers. To differentiate the SAPC PCF, the original SAPC is called the SAPC PCRF which performs policy and charging controls related to 4G subscribers. The term SAPC before SAPC 1.10.0 refers to the SAPC PCRF only, and from SAPC 1.10.0 up refers to both PCRF and PCF.

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 Virtual Network Function (VNF) in a standalone configuration, using internal repository, in the following network environments:

- **Scenario A**, where the SAPC PCRF uses the Gx Rel 9 interface towards GGSN. Default Bearer QoS Control is activated.
- **Scenario B1**, where the SAPC PCRF uses the 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 PCRF uses Gx Rel 9 interface towards Ericsson EPG or with any PDN Gateway.
- **Scenario F1**, IMS VoLTE solution
- **Scenario H**, where the SAPC PCRF uses the Smp interface towards Ericsson SGSN-MME
- **Scenario A PCF**, where the SAPC PCF uses N7 interface towards SMF. PDU Session QoS Control is activated.
- **Scenario B1 PCF**, where the SAPC PCF uses the N7 interface towards SMF. PDU Session Qos Control and Usage Reporting are activated.
- **Scenario F1 PCF**, IMS VoLTE solution in SAPC PCF.
- **Scenario H1 PCF**, where the SAPC PCF uses N15 interface towards AMF.
- **Scenario I1 PCF**, where the SAPC PCF uses N7 interface towards SMF and Internal Database. PDU Session QoS Control is activated.
- **Scenario J PCRF/PCF**, where the SAPC PCRF/PCF uses Gx/N7 interfaces. IMS VoLTE.
- **Scenario K PCF**, where the SAPC PCF uses N5/N30 interfaces towards NEF.

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

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

Note: Simultaneous Attached User is the number of Simultaneous Attached User provisioned in the node.

Scenario A: Gx, QoS

— 0.34 Default IPCAN bearer establishment per Simultaneous Attached User during the Busy Hour

— 0.34 Default IPCAN bearer release per Simultaneous Attached User during the Busy Hour

— 1 Gx Interim per session

— 1 session per Simultaneous Attached User

Scenario B1: Gx, QoS, Usage Reporting

— 0.34 Default IPCAN bearer establishment per Simultaneous Attached User during the Busy Hour

— 0.34 Default IPCAN bearer release per Simultaneous Attached User during the Busy Hour

— 1 Gx interim per session

— 0.3 Default IPCAN session modification owing to Usage Reporting for Mobile per session

— 100% of the subscribers use Usage Reporting for Mobile function

— 0.5 IPCAN session per Simultaneous Attached User

Scenario F: LTE/EPC Solution

— 0.2 IPCAN session establishment per Simultaneous Attached User during the Busy Hour

— 0.18 IPCAN session release per Simultaneous Attached User during the Busy Hour

— 2.5 IPCAN sessions interim per IPCAN session during the Busy Hour

— 1 IPCAN session per Simultaneous Attached User

Scenario F1: IMS VoLTE Solution

— 0.2 IPCAN session establishment per Simultaneous Attached User during the Busy Hour

— 0.18 IPCAN session release per Simultaneous Attached User during the Busy Hour

- 2.5 IPCAN sessions interim per IPCAN session during the Busy Hour
- 1 IPCAN session per Simultaneous Attached User
- 1.43 AF session establishment per Simultaneous Attached User during the Busy Hour
- 1.43 AF session modification per Simultaneous Attached User during the Busy Hour
- 1.43 AF session release per Simultaneous Attached User during the Busy Hour
- 100% of the subscribers use VoLTE services
- The average duration per AF session is 1.5 minutes

Scenario H: Smp

- 1 IPCAN session per Simultaneous Attached User
- 2 number of cell changes reported over S1-MME per Simultaneous Attached User per Busy Hour
- 0.1 number of Smp session update initiated by MME per Simultaneous Attached User per Busy Hour
- 2 number of location changes reported over Iu-SGSN per Simultaneous Attached User per Busy Hour
- 0.1 number of Smp session update initiated by SGSN per Simultaneous Attached User per Busy Hour

Scenario A PCF: N7, QoS

- 0.34 PDU session establishment per Simultaneous Attached User during the Busy Hour
- 0.34 PDU session release per Simultaneous Attached User during the Busy Hour
- 1 N7 Interim per session
- 0.5 session per Simultaneous Attached User

Scenario B1 PCF: N7, QoS, Usage Reporting

- 0.34 PDU session establishment per Simultaneous Attached User during the Busy Hour

- 0.34 PDU session release per Simultaneous Attached User during the Busy Hour
- 1 N7 interim per session
- 100% of the subscribers use Usage Reporting for Mobile function
- 0.5 session per Simultaneous Attached User

Scenario F1 PCF: IMS VoLTE Solution

- 0.34 PDU session establishment per Simultaneous Attached User during the Busy Hour
- 0.34 PDU session release per Simultaneous Attached User during the Busy Hour
- 1 PDU session interim per PDU session during the Busy Hour
- 1 session per Simultaneous Attached User
- 1.43 AF session establishment per Simultaneous Attached User during the Busy Hour
- 1.43 AF session modification per Simultaneous Attached User during the Busy Hour
- 1.43 AF session release per Simultaneous Attached User during the Busy Hour
- 100% of the subscribers use VoLTE services
- The average duration per AF session is 1.5 minutes

Note: As the 5GC standard requirement, the subscribers are provisioned in the Unified Data Repository (UDR).

Scenario I1 PCF: N7, QoS, Internal Database

- 0.34 session establishment per Simultaneous Attached User during the Busy Hour
- 0.34 session release per Simultaneous Attached User during the Busy Hour
- 1 N7 Interim per session
- 0.5 session per Simultaneous Attached User

Note: The subscribers are provisioned in the Internal Database.

Scenario J PCRF/PCF: IMS VoLTE

- 0.2 Default IPCAN bearer establishment per subscriber during the Busy Hour
- 0.18 Default IPCAN bearer release per subscriber during the Busy Hour
- 2.5 Gx Interim per session
- 1 session per subscriber
- 0.4 PDU session establishment per subscriber during the Busy Hour
- 0.36 PDU session release per subscriber during the Busy Hour
- 2.5 PDU sessions interim per PDU session during the Busy Hour
- 2 sessions per subscriber
- 1.43 AF session establishment per subscriber during the Busy Hour
- 1.43 AF session modification per subscriber during the Busy Hour
- 1.43 AF session release per subscriber during the Busy Hour
- 10% of the subscribers use VoLTE services
- The average duration per AF session is 1.5 minutes

Scenario K PCF: N5/N30, Exposure

- 0.34 PDU session establishment per Simultaneous Attached User during the Busy Hour
- 0.34 PDU session release per Simultaneous Attached User during the Busy Hour
- 1 PDU session interim per PDU session during the Busy Hour
- 0.34 AF Session establishment with Required QoS per Simultaneous Attached User during the Busy Hour
- 0.34 AF Session release with Required QoS per Simultaneous Attached User during the Busy Hour
- 1 AF Session update with Required QoS per PDU session during the Busy Hour
- 0.5 session per Simultaneous Attached User
- 100% of the subscribers use Exposure services
- The average duration per AF session is 1.5 minutes

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.

— Subscriber Profile used for 5G scenarios: 14 authorized services in the N7 interface per PDU 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 and for the N7 interface when executing similar functions is about the same.

Moreover, the maximum Subscriber Capacity, and the maximum Transactions Per Second of SAPC PCF per each network scenario are shown.

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

Logging level has been increased to level 6. This can affect to the node performance.

Table 1 Scenario A: Gx, QoS

Scenario A	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	5.7	48.1	93.9	292.8
Transactions Per Second	1133	9549	18617	58078
PDP Sessions (thousands)	2000	16851	32854	102490

Table 2 Scenario B1: Gx, QoS, Usage Reporting

Scenario B1	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	4.4	37.0	72.2	225.2
Transactions Per Second	957	8066	15726	49060
PDP Sessions (thousands)	1538	12963	25274	78846

Table 3 Scenario F: LTE/EPC Solution

Scenario F	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	6.7	56.3	109.8	342.5
Transactions Per Second	1143	9636	18788	58611
Number of Gx sessions (thousands)	4678	39422	76860	239771

Table 4 Scenario F1: IMS VoLTE Solution

Scenario F1	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	0.8	7.3	14.2	44.3
Transactions Per Second	869	7328	14286	44568
Number of Gx sessions (thousands)	605	5102	9948	31033
AF Sessions (thousands)	22	182	355	1109

Table 5 Scenario H: Smp

Scenario H	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	8.6	72.7	141.7	442.2
Number of IPCAN sessions using Smp (thousands)	6039	50889	99218	309518
Transactions Per Second	1812	15267	29765	92855

Table 6 Scenario A PCF: N7, QoS

Scenario A PCF	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	3.7	31.5	59.6	199.6

Scenario A PCF	2 TP	10 TP	20 TP	67 TP
Transactions Per Second	745	6238	11818	39589
PDU Sessions (thousands)	2234	18713	35453	118765

Table 7 Scenario B1 PCF: N7, QoS, Usage Reporting

Scenario B1 PCF	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	2.4	20.2	38.2	128.1
Transactions Per Second	525	4396	8328	27900
PDU Sessions (thousands)	1433	12011	22754	76224

Table 8 Scenario F1 PCF: IMS VoLTE Solution

Scenario F1 PCF	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	0.6	4.9	9.3	31.3
Transactions Per Second	608	5094	9650	32326
PDU Sessions (thousands)	350	2935	5561	18629
AF Sessions	14	124	234	783

Table 9 Scenario H1 PCF: N15 Solution

Scenario H1 PCF	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	1.8	15.6	29.7	99.4
Transactions Per Second	584	4889	9262	31029
N15 Sessions (thousands)	1308	10955	20754	69525

Table 10 Scenario I1 PCF: N7, QoS, Internal Database

Scenario I1 PCF	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	3.4	28.5	54	180.9
Transactions Per Second	783	6566	12441	41677
PDU Sessions (thousands)	4032	33779	63995	214381

Table 11 Scenario J PCRF/PCF: Gx/N7, IMS VoLTE

Scenario J PCRF/ PCF	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	0.6	5.1	9.8	31.6
Gx Transactions per Second	53	449	876	2730
N7 Transactions Per Second	59	490	926	3105
Rx Transactions Per Second	505	4246	8165	26368
Number of Gx sessions (thousands)	108	918	1790	5584
PDU Sessions (thousands)	87	733	1390	4657
AF Sessions	15	128	245	791

Table 12 Scenario K1 PCF: N5/N30, Exposure

Scenario K1 PCF	2 TP	10 TP	20 TP	67 TP
Millions of Subscribers	0.5	4.2	8	26.8
Transactions per Second	549	4602	8720	29211
PDU Sessions (thousands)	300	2510	4756	15933

Scenario K1 PCF	2 TP	10 TP	20 TP	67 TP
AF Sessions (thousands)	449	3766	7135	23900

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 an external database, which needs a write operation to the external database.

— 10% reduction in the number of TPS supported, when no accumulators are stored in the external database.

2.1.2 Performance Impact by Policies, Rules and Conditions

The number and complexity of the policies, rules and conditions which are configured and used in different operations of the SAPC node might have a big impact on the performance in term of TPS at a given CPU load. For example:

— If the number of conditions is larger than 300 for Gx traffic, then the impact is significant (20% TPS reduced), which is compared with 10 conditions as base.

— If the number of rules is larger than 100 for Smp traffic, then the impact is significant (40% TPS reduced). If the number of rules is larger than 300, then 70% TPS is reduced. The comparison base is 1 rule.

To obtain optimized node performance, observe the following recommendations:

— Configure a number of rules and conditions as small as possible.

— For Gx traffic, the weight of number of conditions is heavier than the weight of number of rules.

— For Smp traffic, the weight of number of rules is heavier than the weight of number of conditions.

Note: To obtain specific figures of reduced TPS at a given CPU load when configuring a large number of rules or conditions, dimensioning exercise is highly recommended.

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 IP Network Design on page 21.

2.3.3 SAPC 1.2

From SAPC 1.2 onwards, the SAPC SW package format follows the Ericsson standard CSM (CBA SW Model). It is a unified model, for installation and upgrade packages that simplifies the SW management in the node.

Attention!

Due to this change, the SW upgrade to the SAPC 1.2 version implies a service outage during the rolling upgrade procedure.For further information about upgrade timing and impacts refer to SAPC Upgrade Information.

2.3.4 SAPC 1.3

The SAPC provides an upgrade method for the SAPC Virtual Network Function (VNF) in standalone scenarios.

The Upgrade by Replacement procedure is based on the whole VNF replacement. It provides a smooth upgrade process as it has no impact on other telecom network nodes, and it does not cause any service outages, because both SAPC VNF instances with the old and the new SAPC versions are deployed simultaneously during the upgrade procedure.

The prerequisite of this upgrade procedure is to provide SAPC with the following:

- The provision of virtual resources in the data center to allow the deployment of the two SAPC VNF instances during the upgrade procedure.
- Two extra virtual IP (VIP) addresses for Operation and Maintenance (OAM) access during the upgrade procedure.
- Two extra VIP addresses for dynamic data replication during the upgrade procedure.

2.3.5 SAPC 1.4

For the SAPC PNF upgrade, if the hardware used is NSP 6.1 with GEP3 blades, the validated and mandatory GEP3 firmware version to ensure a successful upgrade is R11A or later.

The GEP3 firmware version must be updated as a pre-upgrade step.

GeoRed soaking period time frame can be extended, so nodes running different SAPC versions can synchronize during normal operation.

2.3.6 SAPC 1.7

The upgrade by replacement procedure for VNF stand-alone deployments is updated to allow scenarios in which the diameter payload traffic in the destination SAPC vAPP is configured to use Stream Control Transmission Protocol (SCTP) Multi-Homing with Path Diversity.

2.3.7 SAPC 1.8

The upgrade by replacement procedure for VNF deployments is updated to allow Active-Active Geographical Redundancy scenarios. All the configuration changes supported previously via upgrade by replacement limited for Stand-Alone scenarios can now be applied also for Active-Active Geographical Redundancy.

2.3.8 SAPC 1.9

The upgrade by replacement procedure for VNF deployments is updated to allow Active-Standby Geographical Redundancy scenarios. All the configuration changes supported previously via upgrade by replacement can now be applied also for Active-Standby Geographical Redundancy.

The upgrade script provided by the SAPC can be executed from the system controller as well as from an external machine. Both methods of procedure, running the upgrade script from an external machine or from the system controller are allowed.

2.3.9 SAPC 1.11

— For the SAPC VNF upgrade procedure, a smooth upgrade is ensured if TLS is enabled for the SAPC. For more information, refer to SAPC Upgrade Instruction.

— The upgrade by replacement procedure for VNF deployments is updated to ensure a smooth upgrade if TLS is enabled in the origin SAPC and the certificates are issued by a trusted Certificate Authority (CA).

2.3.10 SAPC 1.12

Due to the SAPC supports IP address Overlapping for the SMF, the SW upgrade to the SAPC 1.12 version causes partial N7 traffic failure during the rolling upgrade procedure.

2.3.11 SAPC 1.13

Upgrade procedure is modified to remove the step for Memory dimensioning in PLs as the correspondent procedure has been removed.

2.3.12 SAPC 1.14

The Upgrade by Replacement procedure is deprecated from SAPC 1.14 onwards.

2.3.13 SAPC 1.15

— Single Step upgrade is recommended to avoid cases of SM or AM Policy Association URI mismatching that is possible to happen if Rolling upgrade is used, as is explained in *Description of Impacts* of SAPC PCF Support for FQDN on page 138.

— The upgrade procedure has been improved to consider the increase of memory of the PL VMs in SAPC VNF. Refer to *Memory Dimensioning in PLs* in the SAPC Upgrade Instruction document for more information.

— The new PCF functionality and architectural changes have a performance impact on SAPC, with the measured impact being as below:

  — 4G traffic shows a performance decrement of around 11% for GX and 6% for RX.

  — 5G traffic shows a performance decrement of around 15% for both N7 and Rx.

2.3.14 SAPC 1.18

— The hardware requirement for upgrade is changed to: at least 12 GB of free space in mounted hard disk at `/cluster`.

— If the node uses the ECS certificate for NELS and an upgrade to version SAPC1.18 is going to be performed, it is necessary to use the EPPKI certificate before applying the upgrade.

2.3.15 SAPC 1.19

SAPC PCF Integration with OCS, for AM or UE Policy Control in SAPC 1.19

The introduction of SAPC PCF Integration with OCS, for AM or UE Policy Control in SAPC 1.19 have impacts to the following functions:

— Addition of Location AVPs to 3GPP Sy Interface

  If an AM policy association session over N15 interface is established firstly, the Sy session is established with the 3GPP-SGSN-MCC-MNC AVP on the condition that the `userLoc` is received. If a UE policy association session over N15 interface is established firstly, the Sy session is established without any location-related information because the SAPC PCF does not support `userLoc` in UE policy association.

— AM (N15) and SM (N7) Joint Policy Evaluation

  To keep the same behavior as before when integrating with OCS, it is required to get the same traffic Ids from N15 AM policy association session as N7 sessions, or it is required to be able to get the same information from OCS by different traffic Ids (MSISDN, IMSI(s)) of the same subscriber.

SAPC PCF recoveryTime Support in pcfBinding Improvement

The prerequisites of this upgrade procedure are as the following:

— The SAPC PCF is interworking with the Binding Support Function (BSF).

— The SAPC PCF restart detection function is enabled by the BSF based on the `recoveryTime` in the `pcfBinding` data structure.

— The start or last restart of SAPC happens during the daylight saving time of local time zone.

To restart SAPC, apply Single Step upgrade:

— for standalone deployment, perform with SAPC restart.

— for Active-Standby/Active-Active Geographical Redundancy deployment, perform with both SAPC peers restart simultaneously.

After the restart, all the existing sessions will be lost in SAPC. The new recovery time of SAPC will be sent to the BSF to indicate the SAPC restart, and the BSF can clean up all the sessions established before the SAPC restart. For more information, see SAPC PCF recoveryTime Support in pcfBinding Improvement on page 178.

2.3.16 SAPC 1.20

— Before using Workflow for SAPC upgrade, the minimum available disk space shall be checked. It's stated starting from SAPC 1.20, but it's also applicable for all previous releases.

  For details, refer to *Upgrade SAPC* in SAPC VNF Lifecycle Manager Workflow Instruction for OpenStack.

— One improvement of Workflow for reducing disk space usage during SAPC upgrade is delivered.

  For details, refer to *Upgrade Failure due to Lack of Disk Space* in Workflows Troubleshooting Guide.

2.3.17 SAPC 1.20CP1

— The SAPC 1.120 CP1 VNF performs around 4% less TPS for 5G SMF and 5G Voice respectively than the SAPC 1.20 VNF, which is caused by CBA uplift (GCC 10.3 introduced). While 4G Traffic performance is similar to SAPC 1.20.

— From EVNFM 24.0.0 onwards, the pre-TOSCA workflow is no longer supported. If the pre-TOSCA workflow is used and the EVNFM is upgraded to 24.0.0 or later version, the migration from pre-TOSCA to TOSCA should be executed. For details, refer to SAPC VNF Lifecycle Manager Workflow Instruction for TOSCA Deployments.

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

2.4.3 SAPC 1.2

When the SAPC is deployed as part of the User Data Consolidation (UDC) solution and Session Context Exposure is enabled (disabled by default), consider the following impacts:

— Application schema in CUDB:

  • Added `OngoingSession` and `ClosedSession` attributes in a new object class `SAPC5`.

2.4.4 SAPC 1.4

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

Do!

Disable the **Local Reads** feature in the CUDB in order to secure data consistency in scenarios in which the SAPC is writing data to the CUDB enabling the SAPC to always read the most up-to-date value.

2.4.5 SAPC 1.5

When the SAPC is deployed as part of the UDC solution, consider the following impacts:

— Application schema in CUDB:

- Added `CDC` attribute in the SAPC object class.
- Added `FamId`, `GrpId`, `Acum` and `CDC` attributes in a new object class `SAPC4`.
- Added `GrpId`, `Gprio`, `StartD` and `EndD` attributes in the object class `SAPC3` under the object class `SAPC4`.

2.4.6 SAPC 1.12

When the SAPC is deployed as part of the User Data Consolidation (UDC) solution, and CCDM (instead of CUDB) is used as external database for SAPC PCRF, consider the following impacts:

— Application counters in CCDM:

- New file `SAPC Application Counters Configuration for CCDM` provided for configuring SAPC applications counters in CCDM.

— Notification files with CCDM:

- New file `SAPC SOAP Notifications Configuration for CCDM` provided for configuring SOAP notifications in CCDM.

For more information refer to Configuration Guide for SAPC Application in UDC.

2.4.7 SAPC 1.15

When the SAPC is deployed as part of the User Data Consolidation (UDC) solution, and CUDB is used as external database for SAPC, consider the following impacts:

— The installation/uninstallation script of SAPC application counters is enhanced to support both encrypted and non-encrypted MySQL password in the CUDB, where the encrypted MySQL password is introduced in CUDB 1.23. To manage SAPC application counters in CUDB 1.23 or later version, use the *Integration in UDC solution* package from SAPC 1.15 or later version and apply it in CUDB.

2.5 Changes in Maintenance and Troubleshooting

2.5.1 BackupFormatter Tool

Introduced in: SAPC 1.1

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

2.5.2 EBM Data Parsing Tools

Introduced in: SAPC 1.4

The Event-Based Monitoring (EBM) stream recorder tool (`ebm_stream_recorder` or `ebm_stream_recorder64`) can be used to record streamed EBM data into a binary EBM log file.

The EBM decoder tool (`parse_ebm_log.pl`) can be used to parse binary EBM log files into readable text files.

2.5.3 Packet Capture Tool

Introduced in: SAPC 1.7

The Packet Capture Tool (`sapcCaptureTool`) can be used to capture traffic from the live PL nodes of the SAPC. The collected data can be used for maintenance. For more information, see SAPC Troubleshooting Guide.

2.5.4 SAPC Collect Info Improvement

Introduced in: SAPC 1.9

— The SAPC Collect Info tool (`sapcCollectInfo`) has been updated to collect further information.

— Other minor improvements have been implemented, such as the execution of the script with low I/O and CPU priority (to avoid performance impact on live nodes).

— The collected output (on the generated compressed file) is now stored using a different directory structure.

For more information, refer to the Data Collection Guideline for SAPC document.

2.5.5 Measures

2.5.5.1 DBS and LDE Measures

Introduced in: SAPC 1.9

Support of new counters provided by DBS.

Enhance resource counters with complete set of LDE counters for CPU Load and Memory.

2.5.5.2 LEM Measures

Introduced in: SAPC 1.15

Support of counters provided by LEM in the OsmPI, OsmPLU, OsmPU PM Groups.

Enhance troubleshooting by collecting more node information.

2.5.6 Default Backups

Introduced in: SAPC 1.9 EP1

The default number of backups is reduced to 5 each from 100. In this configuration, if more than 5 backups are available and the operator creates a new one, the oldest backups are deleted automatically and only 5 backups remain in the SAPC. The `autoDelete` attribute must be set to `Enabled` for the automatic deletion to occur.

2.5.7 sapcRestExport

Introduced in: SAPC 1.10

The `sapcRestExport` script collects Provisioning Information from the SAPC Rest server. Refer to the Data Collection Guideline for SAPC document for further information about this command.

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!

These improvements can be applied only through upgrade by replacement or new deployment. See Changes in Upgrade Procedure chapter for upgrade by replacement support details.

— 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.
- For standalone and Active-Active Geographical Redundancy deployments, OSPF in the external network is not required, therefore, if static routes are configured for external network connectivity, the OSPF area 0 is created in a new interlink between both VRs, and the VRRP address between VRs should be set. For Active-Standby Geographical Redundancy deployments, OSPF in the external network is mandatory, therefore, VRRP in VRs should not be configured. Refer to the *VirtualRouters* section of the *Adapt Cluster Tool Configuration File* for specific parameters.
- The software of the Virtual Routers is updated to include a new version of the VMware Tools.

Attention!

These improvements can be applied only through upgrade by replacement or new deployment. See Changes in Upgrade Procedure chapter for upgrade by replacement support details.

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.
- IP addresses used previously for SCs (sapc_internal_sp network) are reassigned in the SCXB for ARP monitoring:
  - .1 for SCXB-0-0 (left).
  - .2 for SCXB-0-25 (right).
- Additional IP addresses from the sapc_internal_sp are now assigned to the SCs in the Network:
  - .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.

Note: These improvements only apply to new deployments.

— Deployment recommended 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.

2.6.2 SAPC 1.2

Physical traffic separation can be configured for OAM and Provisioning.

Attention!

These improvements can be applied only through upgrade by replacement (available only for VNF) or new deployment. See Changes in Upgrade Procedure chapter for upgrade by replacement support details.

VNF deployments with Virtual Routers will be deprecated in the near future, therefore, they are only supported in upgrades from previous SAPC releases for legacy reasons. New VNF deployments must be configured without VRs.

2.6.3 SAPC 1.3

The following features are supported:

— Physical traffic separation can be configured for Event-Based Monitoring (EBM).

— IPv6-only configuration is supported in the external networks for OAM and signalling traffic that permits the communication with SAPC neighbors such as PCEFs, External Databases or Provisioning Systems for both VNF and PNF deployments.

  For PNF, this does not include the hypervisor management network and the BSP Northbound OAM network for PNF deployments, that are supported only with IPv4.

  For VNF, the IPv6-only configuration is supported only for deployments without Virtual Routers.

Attention!

These improvements can be applied only through upgrade by replacement (available only for VNF) or new deployment. See Changes in Upgrade Procedure chapter for upgrade by replacement support details.

2.6.4 SAPC 1.7

2.6.4.1 VNF

The following improvements must be considered for SAPC VNF deployments:

— SCTP Multi-Homing with Path Diversity is supported for VNF deployments without Virtual Routers. For more information, refer to SAPC VNF Network Configuration Guide. For the specific related parameters, refer to Adapt Cluster Tool.

— SCTP Multi-Homing with Single Path can be automatically configured using the Adapt Cluster Tool for VNF deployments without Virtual Routers. Manual configuration is no longer needed. For more information, refer to SAPC VNF Network Configuration Guide. For the specific related parameters, refer to Adapt Cluster Tool.

— The `SCTP_ALB` parameter in the Adapt Cluster Tool for SCTP Single-Homing configuration is replaced by the parameter `SINGLEHOMED_SCTP`. For more information, refer to Adapt Cluster Tool.

— SAPC is able to configure different SCTP FrontEnds for the diameter payload traffic. Each traffic can be handled by any of the supported SCTP configurations:

  - Single-Homing
  - Multi-Homing with Single Path

- Multi-Homing with Path Diversity

— For scenarios in which the SAPC is acting as a client (Sy/Sd) and SCTP is used as transport configuration for those traffics, the VIP address or VIP addresses for the SAPC as a client must be configured, together with the Abstract Load Balancer (ALB), which is used to publish them. This is applicable for Single-Homed and Multi-Homed SCTP scenarios. Additionally, for Multi-Homed SCTP, the `OtpdiaHost` object containing the configuration of the remote endpoints (Online Charging System (OCS) for Sy, Traffic Detection Function (TDF) for Sd) must include the two correspondent IP addresses. For more information, refer to Configuration Guide for Diameter.

— Dual-Stack configuration is supported for the External Networks to allow the interaction with the surrounding network elements using IPv4 and IPv6 traffic simultaneously. This support is available for VNF deployments without Virtual Routers. For more information, refer to SAPC VNF Network Configuration Guide. For the specific related parameters, refer to Adapt Cluster Tool.

Note: These improvements can be applied only through upgrade by replacement or in a new deployment. For details about upgrade by replacement, see Changes in Upgrade Procedure on page 12.

2.6.4.2 PNF

The following changes must be considered for SAPC PNF deployments:

— The `SCTP_ALB` parameter in the Adapt Cluster Tool for SCTP Single-Homing configuration is replaced by the parameter `SINGLEHOMED_SCTP`. For more information, refer to the Adapt Cluster Tool document.

— It is possible to configure the SAPC with different SCTP FrontEnds for the diameter payload traffic.

— For scenarios in which the SAPC is acting as a client (Sy/Sd) and SCTP is used as transport configuration for those traffics, the VIP address or VIP addresses for the SAPC as a client must be configured, together with the Abstract Load Balancer (ALB), which is used to publish them. For more information, refer to the Configuration Guide for Diameter document.

Note: These improvements only apply to new deployments.

2.6.5 SAPC 1.8

2.6.5.1 PNF

The following improvements must be considered for SAPC PNF deployments:

— Dual-Stack configuration is supported for the External Networks to allow the interaction with the surrounding network elements using

IPv4 and IPv6 traffic simultaneously. This support is available for the following PNF deployments: NSP6.1 and BSP 8100. Refer to BSP 8100 Network Configuration Guide for more information. For the specific related parameters, refer to the Adapt Cluster Tool document. This configuration is only available for new deployments.

2.6.6 SAPC 1.9

2.6.6.1 VNF

Networking scenarios including Virtual Routers VMs within the SAPC cluster are removed as this deployment type is deprecated. For existing deployments with this configuration, a procedure based on the upgrade by replacement method is provided to migrate to new deployments without Virtual Routers.

2.6.7 SAPC 1.10 with Limited Availability

2.6.7.1 VNF

The following impact must be considered for the SAPC PCF functionality:

— The configuration of traffic IP for the SAPC PCF is the same as for the SAPC PCRF network. All traffic Service Based Interfaces (SBIs) use the same set of IP addresses.

— Traffic separation is supported for HTTP/2 interface, including N7, N36, and Nnrf. For more information, see Adapt Cluster Tool.

2.6.8 SAPC 1.11

Everything under SAPC 1.10 with Limited Availability on page 26 is provided with General Availability in SAPC 1.11.

The network range of FEE networks for both IPv4 and IPv6 are limited up to 255 hosts, meaning that 24 would be the wider (maximum) mask for IPv4 and 120 for IPv6 networks. Refer to *_FEE_NETWORK parameters in Adapt Cluster Tool.

2.6.8.1 VNF

The following improvements must be considered for SAPC PCF functionality:

— Dual-Stack is supported for SAPC PCF functionality to allow the interaction through HTTP/2 interface, including N7, N36 and Nnrf, using IPv4 and IPv6 traffic simultaneously. For more information, refer to SAPC VNF Network Configuration Guide. For information about specific related parameters, refer to Adapt Cluster Tool.

The following improvements must be considered for the SAPC VNF deployments:

— The default configuration of floating FEE nodes in PLs can be modified to fixed. For more information, refer to SAPC VNF Network Configuration Guide and Adapt Cluster Tool.

— Fixed IP Addresses can be set for the ports attached to the External Networks in SCs and PLs for deployments in OpenStack using HOT descriptors. For more information, refer to SAPC VNF Descriptor Generator Tool.

Note: These improvements can be applied only through upgrade by replacement or new deployment. See Changes in Upgrade Procedure on page 12 for upgrade by replacement support details.

2.6.9 SAPC 1.13

2.6.9.1 VNF

The following improvements must be considered for SAPC VNF deployments:

— VLAN-based traffic separation for SAPC External Networks is allowed for VNF deployments in OpenStack (HOT/CSAR packages) and VMware environments (OVF/CSAR packages). This configuration can be applied through upgrade by replacement or new deployment. See Changes in Upgrade Procedure on page 12 for upgrade by replacement support details.

— A new document is provided on how to separate traffic in a live SAPC deployed with VLAN-based configuration. It is important to remark that this document is only a guideline, that is, the specific steps required in each deployment must be detailed by the Customer Units as part of a system integration project. Refer to Add VLAN-based traffic separation to a Live SAPC.

2.6.10 SAPC 1.14

2.6.10.1 VNF

The following improvements must be considered for SAPC VNF deployments:

— SAPC is able to define Network QoS related parameters in its VNF-D for OpenStack deployments. For more information, refer to SAPC VNF Network Configuration Guide and SAPC VNF Descriptor Generator Tool. Additionally, a new document, Change Network QoS in VNF-D for a Live SAPC in OpenStack, is provided regarding how to add or modify these parameters in a live SAPC.

— The parameter `heat_template_version` in VNF-D describing the Heat Orchestrator Template (HOT) version is now configurable in the Descriptor Generator Tool. For further information, refer to SAPC VNF Descriptor Generator Tool.

2.6.10.2 PNF

SAPC PNF initial installation is deprecated including support and documentation. From this release onwards only upgrade is supported.

2.6.11 SAPC 1.15

2.6.11.1 PNF

SAPC PNF on NSP 6.1 is not supported from these release onwards: neither initial installation (which was already deprecated in SAPC 1.14) nor upgrade is supported.

2.6.12 SAPC 1.16

2.6.12.1 VNF

Geographical Redundancy VNF-PNF mixed setup is supported, not only for migration purposes, but for permanent solutions. SAPC 1.16 deployment is required.

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:

— rxAaasUnknownSessionId

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.

2.7.3 SAPC 1.2

Provisioning REST interface

Provisioning REST interface enhanced to use SecM for TLS supported cipher configuration. The list of recommended enabled TLS cipher suites for the SAPC is specified in SAPC Security User Guide.

2.7.4 SAPC 1.4

Logging Event Related to SAPC REST Operation

The SAPC provides the REST Operation Req failed logging event for the REST operation request failed.

Measurements for Network Traffic

Measurements related to sent or received IPv4 or IPv6 octets and datagrams are provided.

Measurements for Gx Interface

For PCEFs configured as clustered Diameter systems, the PCEF peer identifier reported as Measured Object Instance is the logical node identifier, instead of the `Origin-Host` AVP.

RAM Memory Distribution

The PayLoad root partition size is changed from 4 GB to 5 GB.

SC Abscence Feature enabled by default for new geored deployments

From SAPC 1.4, the SCs absence feature is provided by default in geored deployments for maiden installations. Standalone deployments already supported this feature by default. It allows PLs to handle traffic during 15 minutes with both SCs down before a cluster restart is triggered. For more information, refer to Availability and Scalability Facility Description.

For geored deployments upgrading from older releases, this feature can be manually enabled. Refer to *Core MW Resilience Level Two (RL2)* Function Description.

2.7.5 SAPC 1.5

Logging Events Related to SAPC REST Operation

— A minor change is done to the REST Operation Req failed logging event.

— The REST Operation Req answered logging event is added.

— A new directory is provided to store REST log files.

Note: REST logging events could be dropped when the number of logging events per second (LPS) is high. In configuration of 10 PLs, it is expected that 5% of logging events may be dropped when LPS reaches 4000. At higher rate of LPS, the percentage of lost logging events may be higher.

2.7.6 SAPC 1.6

Mandatory AVP flag in Failed-AVP Content

At reception of a message with diameter protocol error, the answer message sets the `M` bit of the AVP contained in `Failed-AVP` to `0` due to a change in the interpretation of diameter dictionaries.

Support of new counters for IPv4 and IPv6 (provided by eVIP)

Support of new CBA alarms based on thresholds

— The SAPC can now configure alarms that can be triggered based on counter thresholds.

— Specifically, alarms for Diameter connectivity, SCTP congestion (provided by eVIP), and CPU and memory usage (provided by LDE) can be configured.

New eri-ipmi tool

— This tool provides useful HW information to GEP Support, enabling the confirmation or not of any HW issues in the SCs.

— The SAPC SW delivery now provides the `eri-ipmi` tool installed in the PNF Hosts.

New alarms for System Resources Monitoring

— Alarms are provided to monitor the CPU usage at cluster level: SRM Alarm System Resources High Usage and SRM Alarm System Resources Low Usage.

SAPC Informational Logging

— Support of new informational logs using a new syslog-based logging system and support of individual log configuration to enable log severity adjustment and to allow disabling logs.

  Using the Informational logging feature, especially when Logging Level 6 is enabled, may severely impact the CPU load in the SC and the NFS. For this reason, it is highly recommended to activate Logging Level 6 during low-traffic hours and only for short periods of time. For more information, refer to the Logging Events document.

2.7.7 SAPC 1.8

2.7.7.1 REST Counters

The following counters have been introduced in SAPC 1.8:

restGet	The number of REST messages with a GET operation received.
restPut	The number of REST messages with a PUT operation received.
restDelete	The number of REST messages with a DELETE operation received.

2.7.7.2 Logging Level

The default value of the logging level is 4.

2.7.8 SAPC 1.9

2.7.8.1 LDEwS NFS Logger

LDEwS NFS Logger feature is disabled by default to avoid worsen NFS performance under transient overload conditions.

2.7.9 SAPC 1.10

2.7.9.1 New Policy Engine Functions

- `dateToTimestamp(string date)`
- `timestampToDate(integer timestamp)`
- `strToLower(string st)`

For more information, see Configuration Guide for Subscription and Policies.

2.7.9.2 RAM Distribution

The PayLoad root partition size is changed from 5 GB to 6 GB. The change applies both for initial installation and upgrade.

2.7.10 SAPC 1.11

2.7.10.1 New Counters for DIAMETER_USER_UNKNOWN Messages

The following counters have been introduced:

- `gxCcasUserUnknown`
- `gxRaasUserUnknown`
- `sySlasUserUnknown`
- `smpCcasUserUnknown`
- `smpRaasUserUnknown`
- `sdTsasUserUnknown`
- `sdRaasUserUnknown`

2.7.10.2 New Logging Events for N7 Interface

The following logging events have been introduced:

- Error sending HTTP Request over N7 interface
- Error sending HTTP Response over N7 interface
- Timeout receiving Response over N7 interface

2.7.10.3 New Policy Tags

— The following new policy tags are added for session management policy control of the SAPC PCF.

- `AccessData.subscriber.locationInfo.gNbId`
- `AccessData.subscriber.locationInfo.ngeNbId`
- `AccessData.smPolicyContextData.smfId`

— The following existing policy tags are enabled to be used for session management policy control of the SAPC PCF.

- `AccessData.subscriber.locationInfo.anGwIpAddress.v4`
- `AccessData.subscriber.locationInfo.anGwIpAddress.v6`
- `AccessData.userEquipmentInfo.model`
- `AccessData.userEquipmentInfo.serialNr`
- `AccessData.userEquipmentInfo.version`

— The following tag is added for operator specific information:

- `Subscription.OSI["osiName"]`, which is applicable for both 4G and 5G subscribers.

2.7.10.4 New Policy Engine Function

The `isBeforeCurrentBillCycle(string date, string bill-cycle, integer ue-timezone)` function is added.

2.7.11 SAPC 1.12

2.7.11.1 New Alarm

Policy Control, Connection to NRF Failed

2.7.11.2 RAM Distribution

The PayLoad root partition size is changed from 6 GB to 7 GB. The change applies both for initial installation and upgrade.

2.7.12 SAPC 1.13

2.7.12.1 New Counters

The SAPC supports measuring the average latency, the number of transactions that latency is in a time range, and the max latency for the following transactions:

- Receive an Rx AAR (including AAR-I, AAR-U, and PCSCF_RESTORATION) and send a corresponding Rx AAA.
- Receive an Rx AAR (including AAR-I and AAR-U) and send a corresponding Gx RAR.
- Send an Rx ASR and receive a corresponding Rx ASA.
- Send an Rx RAR and receive a corresponding Rx RAA.
- Receive an Rx STR and send a corresponding Rx STA.
- Receive a Gx CCR (including CCR-I, CCR-U, and CCR-T) and send a corresponding Gx CCA.
- Send a Gx RAR and receive a corresponding Gx RAA.
- Send an Sy SLR and receive a corresponding Sy SLA.
- Receive an Sy SNR and send a corresponding Sy SNA.
- Send an Sy STR and receive a corresponding Sy STA.
- Receive an Sd CCR (including CCR-U and CCR-T) and send a corresponding Sd CCA.
- Receive an Sd CCR (including CCR-U) and send a corresponding Gx RAR.
- Send an Sd RAR and receive a corresponding Sd RAA.
- Send an Sd TSR and receive a corresponding Sd TSA.

The following counters are added for the Access and Mobility Management Function (AMF):

- NpcfAmCreateRequests
- NpcfAmCreateFailed
- NpcfAmCreateSuccess
- NpcfAmUpdateRequests
- NpcfAmUpdateSuccess

- NpcfAmUpdateFailed
- NpcfAmDeleteRequests
- NpcfAmDeleteSuccess
- NpcfAmDeleteFailed
- NpcfAmUpdateNotifyRequests
- NpcfAmUpdateNotifySuccess
- NpcfAmUpdateNotifyFailed
- NpcfAmRespFailed
- NpcfAmUserUnknown
- NpcfAmErrorRequestParameters
- AmfActiveSessions

The following counters are added for the Binding Support Function (BSF):

- NbsfDeregisterFailed
- NbsfDeregisterRequests
- NbsfDeregisterSuccess
- NbsfRegisterFailed
- NbsfRegisterRequests
- NbsfRegisterSuccess

For detailed information about the latency measures, refer to Measurements.

2.7.12.2 New Alarms

The following alarms are added:

- Policy Control, Connection to BSF Failed for SM Policy Control
- Policy Control, Failover Caused by Failure on BSF Connection for SM Policy Control
- Policy Control, Number of Nbsf_Management_Register failure Reached
- Policy Control, Failover Caused by Failure on UDR Connection for AM Policy Control

— Policy Control, Connection to UDR Failed for AM Policy Control

— Policy Control, Number of PCF Response Npcf_AMPolicyControl Failure Reached

— Policy Control, Number of PCF Initiated Npcf_SMPolicyControl Update Notify Failure Reached

2.7.12.3 New Key Performance Indicators

The following Key Performance Indicators are added for the AMF:

— NpcfAMCreateFR

— NpcfAMUpdateFR

— NpcfAMUpdateNotifyFR

— NpcfAMDeleteFR

— NpcfAmSessionsFR

— NpcfAMSessionsRate

— AmfActiveSessions

The following Key Performance Indicators are added for the BSF:

— BSF Binding Register Failure Ratio

— BSF Binding Transactions per Second

2.7.12.4 Security Enhancements

SAPC supports 3072 Diffie–Hellman key exchanges in Configuration Management Interface to make system more secured.

New configuration parameter '`dhParamLength`' is added to TLSD Manager Configuration file for application configuration.

It is recommended the usage of the 3072 bits value (consider this for SAPC upgrades), but the operator has to previously assure that all the interworking clients are upgraded or already provide support for it.

Note: For further information refer to *COM 7.15* CPI library.

SAPC provides MD5 Authentication with OSPF. New configuration parameters are added for configuring OSPF MD5 authentication between the Front End Elements and the Gateway Router.

Note: For further information refer to *eVIP 3.16* CPI library.

SAPC implements TLS encryption for the REST interface used to report application information towards NeLS.

It is implemented using only operator layer certificates, ERICSSON layer certificate are not used.

This feature is disabled by default.

Note: For further information refer to *LM 6.14* CPI library.

SAPC supports secure default value for TLS `cipherFilter` attribute (SSLv3 ciphers).

The change is not applied in SAPC upgrades to avoid possible service disturbances in current deployment, but it is recommended to the operator to analyze the new security improvement in order to use it:

— update SEC configuration to avoid the usage of non-secure TLS ciphers)

— and remove value NULL in `cipherFilter` attribute.

Note: For further information refer to *SEC 2.16* CPI library.

2.7.12.5 Operation Enhancements

SAPC provides support for a new basic engine with XPath filter in netconf.

Note: For further information refer to *COM 7.15* CPI library.

SAPC supports Streaming of security logs to a different remote server.

Note: For further information refer to *CoreMW 6.2* CPI library.

SAPC supports a unified log retention housekeeping. The feature is enabled by default and can be disabled from NBI if needed.

Note: For further information refer to *CoreMW 6.2* CPI library.

SAPC supports new path MTU discovery feature for SCTP traffic.

It is possible to enable both 'Path-MTU (PMTU) Discovery' and 'Jumbo Frames' features simultaneously.

Without PMTU Discovery, the MTU has to be set to the smallest size available towards surrounding elements, which makes deployments using jumbo frames on external interfaces restricted when running SCTP traffic.

Note: For further information refer to *SS7CAF 6.13* CPI library.

SAPC allows the definition of a preferred VIP source address to be used for the outgoing traffic in an ALB.

Note: For further information refer to *eVIP 3.16* CPI library.

The CPU Load Peak Threshold Monitoring Job (`cpuLoadPeakThresholdJob`) has been removed to avoid the constant raising and clearing of the corresponding alarm (Performance Management Threshold Crossed or Reached) caused by spontaneous CPU peaks (that are measured as `CPULoad.Total.Maximum`). This change impacts on SAPC Maiden Installations from SAPC 1.13. Otherwise, this operation can be performed manually for SAPC nodes upgraded from earlier versions (refer to Delete Threshold Monitoring Job Operating Instructions).

2.7.12.6 Robustness Enhancements

SAPC triggers a new alarm if log streaming to remote log server fails.

Note: For further information refer to *LDEwS 4.15* CPI library.

SAPC triggers a new alarm to indicate the cloud storage is unavailable.

Alarm contains information of the UUID of the VM and information which volume/disk is problematic.

Note: For further information refer to *LDEwS 4.15* CPI library.

SAPC can configure 2 NeLS IP Addresses to support NeLS in Geographically redundancy mode.

Note: For further information refer to *LM 6.14* CPI library.

2.7.12.7 Troubleshooting Enhancements

SAPC provides new operating option for enabling/disabling front ends.

Note: For further information refer to *eVIP 3.16* CPI library.

2.7.12.8 Diameter Stack Enhancements

Up to SAPC 1.12.0 EP3, C-Diameter (versions 3.4 and below) is not fully compliant with section *6.1.4* of *RFC 6733* as it doesn't check destination host and destination realm of incoming request to correspond with local configuration.

From SAPC 1.13.0, C-Diameter (versions 3.5 and above) complies with section *6.1.4* of *RFC 6733*, so it checks properly destination host and destination realm of incoming requests to correspond with local configuration, and if the check is not OK, the request is answered with Result-Code set to `DIAMETER_UNABLE_TO_DELIVER (3002)`. This standard behavior can be manually disabled if needed by using Diameter initial parameter `DIACC_DIASERVER_MESSAGE_DESTINATION_VALIDATION_ENABLED`.

Note: For further information refer to C-Diameter 3.5 CPI library.

Check the network to know if SAPC Diameter peers are compliant with section *6.1.4* of *RFC 6733* or not. In order to take proper action keep the RFC compliant behavior (option chosen by default after upgrade from SAPC 1.13.0 GA onwards), or disabling this feature to keep backward compatibility.

Procedure to disable RFC compliant behavior is detailed in Upgrade Instruction Document.

2.7.13 SAPC 1.14

2.7.13.1 Operation Enhancements

— 'tipc-config' tool (which is part of tipcutils package) is going to be deprecated in a future SAPC version. Equivalent tool 'tipc' is provided (which is part of iproute2-tipc package). 'tipc' tool provides additional features on top of what 'tipc-config' provides, and has a different user interface.

Recommendation is to avoid using 'tipc-config' and change to use 'tipc'. SAPC documents where 'tipc-config' was referenced have been updated to use 'tipc'.

Note: For further information on 'tipc-config' and 'tipc' tools, refer to *LDE 4.16* CPI library.

2.7.13.2 New Alarms

Following alarms are added:

— Provisioning REST API Unavailable.

2.7.13.3 Configured Severity of CBA Alarms

The severity of the CBA alarms below has been configured with a recommended value in the SAPC using the `configuredSeverity`, instead of the default value provided by CBA (as described in the alarm document).

The configuration is automatically implemented after the SAPC is installed initially, or upgraded if none value is defined before. If a value is defined before, that value is kept after the upgrade.

Table 13 Configured Severity of CBA Alarms

FmAlarmModel	FmAlarmType	configuredSeverity	Alarm Document
SwM	FallbackOperationStartingSoon	Major	A Fallback Operation will soon be started

FmAlarmModel	FmAlarmType	configuredSeverity	Alarm Document
BrM	AutoExportBackupFailed	Minor	BRM, Auto Export Backup Failed
BrM	AutoExportManualBackupFailed	Minor	BRM, Auto Export Manual Backup Failed
BrM	ScheduledBackupFailed	Minor	BRM, Scheduled Backup Failed
CertM	CertMAutomaticEnrollmentFailed	Minor	Certificate Management, Automatic Enrollment Failed
CertM	CertMCertificateNotAvailable	Minor	Certificate Management, a Valid Certificate is Not Available
CertM	CertMCertificateToExpire	Warning	Certificate Management, the Certificate is to Expire
Evip	EvipIPSECTunnelFault	Major	eVIP, IPsec Tunnel Fault
FileManagement	FileMMaxSizeExceeded	Major	File Management, Max Size in FileGroup Exceeded
FileManagement	FileMNoOfFilesExceeded	Major	File Management, Number of Files in FileGroup Exceeded
LOTC	DiskReplicationConsistency	Major	LOTC Disk Replication Consistency
LOTC	MemoryUsage	Major	LOTC Memory Usage
LOTC	TimeSynchronization	Major	LOTC Time Synchronization
Lm	AutonomousModeActivated	Minor	License Management, Autonomous Mode Activated
Lm	EmergencyUnlockResetKeyRequired	Minor	License Management, Emergency Unlock Reset Key Required
Lm	KeyFileFault	Major	License Management, Key File Fault
Lm	LicenseKeyNotAvailable	Major	License Management, License Key Not Available
LocalAuthenticationMethod	LocalAuthNAuthenticationFailureLimitReached	Minor	Local Authentication, Authentication Failure Limit Reached

2.7.13.4 Security Enhancements

— SSH security is improved in SAPC new installations: default deployment configuration does not support weak CBC mode ciphers. If those were needed, SSH `selectedCiphers` could be updated via COM CLI after installation.

This improvement will not apply to SW upgrade. It is encouraged to disable weak CBC ciphers suites. Refer to SAPC Upgrade Instruction doing that.

Note: For further information, refer to *SEC 2.17* CPI library.

— Audit logging configuration and management have been updated in LDEwS:

  • the way to specify customized `auditd` rules is different, the file name of the `auditd` logs is now `/var/log/<SC-Processor>/security_audit`.

This is applicable to a SAPC initial deployment and a SAPC upgrade.

Note: For further information on this feature, refer to *LDEwS 4.16.1* CPI library.

2.7.14 SAPC 1.15

2.7.14.1 New Alarms

Following alarms are added:

— Policy Control, Number of Configuration Error Reached

2.7.14.2 New Counters

The following counter is added for Configuration Error Events:

— `sapcConfigurationError`

2.7.14.3 Troubleshooting Enhancements

SAPC Health Check tool (`sapcHealthCheck`) has been improved to show the CPU & MEM real time status in the output information.

Note: For further information, refer to the SAPC Troubleshooting Guide.

2.7.14.4 RAM Distribution

— For maiden installation, DBS is dimensioned based on the assumption that having a fully filled database, and adding the SAPC memory usage after a fresh install, should not exceed a 70% of total memory, that is:

```
SAPC memory usage after fresh install + DBS total used memory <= 70% of tota →
l memory
```

— The PayLoad root partition size is changed from 7 GB to 8 GB. The change applies both for initial installation and upgrade.

2.7.14.5 Security Enhancements

Default preconfigured rule for protection against TCP SYN flood attacks has been updated to allow a maximum rate of 100 (instead of 10) new connections per second, after a burst of 100 (instead of 10) connections establishment. For more information refer to Security Hardening Guide.

2.7.14.6 Operation Enhancements

— SAPC PCF supports static provisioning of OCS at subscriber level with internalDB.

2.7.15 SAPC 1.16

2.7.15.1 Operation Enhancements

— The SAPC now provides the capability of streaming SAPC logs (application, emergency calls and provisioning logs) towards an external storage system.

  Log entries for all log streams registered with the Log Management Framework can be automatically forwarded to an external storage location. Local logging is disabled if this featured is enabled.

  By default logs are stored in local filesystem.

  The streaming of SAPC application logs can be encrypted using TLS 1.2 as security framework.

  Higher CPU usage in the primary SC can be observed using this feature. Logging reception performance depends on external server characteristics and network latency.

  Note: For further information on this feature, refer to *SAPC 1.16, CorewMw 6.3.0, LDEwS 4.16.1* and *SEC 2.17.0* CPI library.

— `'tipc-config'` tool (which is part of `tipcutils` package) is finally deprecated from SAPC 1.16 version. Equivalent tool `'tipc'` is provided (which is part of `iproute2-tipc` package). `'tipc'` tool provides additional features on top of what `'tipc-config'` provides, and has a different user interface.

  Use `'tipc'` command instead. SAPC documents where `'tipc-config'` was referenced were updated to use `'tipc'` from *SAPC 1.14* CPI library.

  Note: For further information on `'tipc'` tool, refer to *LDE* CPI library.

2.7.15.2 Diameter Stack Enhacements

The SAPC supports fast feedback if no diameter connection is available at message sending. This functionality is enabled by default for upgrades and

maiden installations from SAPC 1.16 release. It is provided by means of the "`DIACC_FAST_FEEDBACK_ENABLED`" configuration attribute set to `true`.

Note: For further information, refer to *C-Diameter 3.10* CPI library.

2.7.15.3 Security Enhacements

— To be compliant with Security Design Rules, SAPC enables by default the non-root execution of LEM and DBS processes.

Note: For further information, refer to *LEM 4.18* CPI library.

— To be compliant with Security Design Rules, SAPC applies strict permission of the linux files and directories, removing global access permission where possible.

Note: For further information refer to *LDEwS 4.18* CPI library.

2.7.16 SAPC 1.17

2.7.16.1 New Policy Tag

The new policy tag `AccessData.receivedServiceType` is added.

2.7.16.2 Logging Events

The following logging events have been adapted for PCF-NRF scenarios:

— Unsuccessful HTTP Response Received

— Timeout receiving HTTP response

— Error sending HTTP response

— Error sending HTTP Request

— HTTP Response Received

— HTTP Request Sent

The following logging events have been introduced:

— HTTP Request Received

— HTTP Response Sent

— PCF Register status change

For detailed information about the logging events, refer to Logging Events.

2.7.16.3 New Alarm

The following alarm has been added for PCF register failure to NRF:

— Policy Control, Registration to NRF Failed

2.7.17 SAPC 1.18

2.7.17.1 Security Enhancements

— From this SAPC version onwards, the `su` command is restricted. `su -` or `sudo` must be used instead.

— From this SAPC version onwards, IMM (cmw-utility immcfg) must be used to manage EvipCommand attributes, instead of using COM, as these attributes have been removed from eVIP MOM, because they needed root permissions.

— Ciphers arcfour and arcfour256 are restricted for SSH connections.

2.7.17.2 License Management

— Application Information will be sent to NeLS by default in an encrypted format through REST interface. If no operator layer certificate is configured, LM will use EPPKI certificates for encryption. This function can be disabled after the upgrade.

  For information regarding disabling the function, refer to the *Disable Application info feature* section in *Configure Application Info to NeLS* for more information.

2.7.17.3 New Policy Engine Function

```
containsByBinarySearch(array list,string elem)
```

For more information, see Configuration Guide for Subscription and Policies.

2.7.17.4 New Policy Tags

The following existing policy tags are enabled to be used for access and mobility policy control of the SAPC PCF:

— `AccessData.userEquipmentInfo.model`

— `AccessData.userEquipmentInfo.serialNr`

— `AccessData.userEquipmentInfo.version`

2.7.17.5 Logging Events

The following logging events have been adapted for PCF-UDR scenarios:

- Unsuccessful HTTP Response Received
- Timeout receiving HTTP response
- Error sending HTTP response
- Error sending HTTP Request
- HTTP Response Received
- HTTP Request Sent
- HTTP Request Received
- HTTP Response Sent

The following logging event has been newly introduced:

- HTTP/2 Connection Lost

For detailed information about the logging events, refer to Logging Events.

2.7.17.6 Origin-State-Id (OSI) Handling

Improved management of OSI for split-brain scenarios on GeoRed Active-Active. Refer to System Administrator Guide for details.

2.7.18 SAPC 1.19

2.7.18.1 Security Enhancements

- New mask is introduced in the node. The new permissions are 027 umask.
- Logs of path `/cluster/storage/no-backup/coremw/var/log/syslog/sapc` can only be read by `root` and `sapcadmin` users.

2.7.18.2 New Alarms

The following CBA alarms are added:

- License Management, License grace period activated
- License Management, Unsuccessful Responses Received Ratio Threshold Crossed

The following alarms related to NF information are added:

— Policy Control, No UDR Peer Node Info

— Policy Control, No BSF Peer Node Info

2.7.18.3 Logging Improvements

— Support to make hostname change persistent in `audit_log_send.confg` to ensure the Node/Host name included in the Audit log message.

2.7.18.4 New Policy Tags

The following existing policy tags are enabled to be used in dynamic OCS selection policy of the SAPC PCF and PCRF:

— Subscriber.x

— Subscriber.groups

— Subscription.OSI["osiName"]

2.7.19 SAPC 1.20

2.7.19.1 New measurements

The following CBA new measurement types are added:

— ip4FragFails

— ip6FragFails

Note: For details, see eVIP 3.25, Ericsson Internal Support.

2.7.19.2 Diameter Stack Enhancements

The enhancements are:

— A new executable script `cdia_bk_plugin.sh` is introduced.

  This script is invoked by LEM component to prevent backup creation in case of faulty or incomplete C-Diameter configuration. This function can be enabled by applying a new initial configuration parameter `DIACC_BK_VETO`, and by default, disabled as the value is not set.

— An improved leader election algorithm based on weight is introduced.

This function can be enabled by applying a new initial configuration parameter `DIACC_DIASERVER_LEADERELECTION_METHOD`, and by default, disabled as the value is not set.

Note: For details, see C-Diameter 3.16, Ericsson Internal Support .

2.7.19.3 Security Enhancements

The enhancements are:

1. The operator must ensure only strong Key Exchange algorithms are used:
   - LDEwS specifies the list of key exchange algorithms recommended by CIS-CAT v3.
2. The operator must ensure SSH AllowTcpForwarding is disabled:
   - LDEwS explicitly disables the usage of the TCP forwarding feature in its `config` files.
3. The operator must ensure SSH MaxStartups is configured:
   - LDEwS specifies the value recommended by CIS-CAT v3.1 in `config` files.
4. Retbleed Vulnerability Mitigation:
   - Retbleed is a variant of Spectre vulnerabilities which exploits the retpoline mitigation. By default, the kernel probes the CPU model and automatically apply the appropriate mitigation for vulnerable CPU.
   - The performance impact of Retbleed mitigation depends highly on the hardware and the built-in mitigation technique. For more information, see SAPC Node Dimensioning Guideline.
   - Retbleed mitigation can be disabled if the user is concerned about the performance impact and accepts the security risk of Retbleed vulnerability, see SAPC Security User Guide.

Note: For details on LDEwS, see LDEwS 4.24, Ericsson Internal Support.

2.7.20 SAPC 1.20CP1

2.7.20.1 License Management

License grace period in NeLS is supported.

Note: For details, see the *LM 6.25* CPI Library.

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 Peer Restart

Introduced in: SAPC 1.0

3.3.1 Description of Impacts

Policy and Charging Enforcement Function (PCEF) restart is detected when any Gx CCR-Initial message is received with an `Origin-State-Id` AVP that is different from the `Origin-State-Id` currently stored in the SAPC. The SGSN-MME restart is also detected in the Smp CCR-Initial and the AF restart is detected in the same way but in any Rx AAR-Initial or AAR-Update messages.

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 does not remove all the sessions established by that peer as done during a peer restart. (Refer to *Massive Gx Clean up* at *PCEF Peer Removal* in Availability and Scalability.)

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 or AAR is received with an `Origin-State-Id` lower than the locally stored one. Any different `Origin-State-Id` is considered for peer restart detection instead.

The reception of missing `Origin-State-Id AVP` (or zero value) is not considered a peer restart by the SAPC. The restart is detected when a new non-zero value `Origin-State-Id` is received different from previous latest non-zero OSI received in the Gx or the Smp client's activation request or in the Rx client's requests (initial or update) for that peer.

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

The following counters are added:

— gxRaasOutOfSpace

— gxRaasPendingTransaction

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.requestedQos.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 SAPC Security User 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 following functions are supported:

- 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.
- SAPC is supported on top of RHOSP.
- Workflows for lifecycle Management through the Virtual Network Function Life Cycle Manager (VNF-LCM) with HEAT are valid for RHOSP deployments.

3.21.2 Interface

Not applicable

3.21.3 Operation

No impact

3.22 Policy Studio Improvements in SAPC 1.2

Introduced in: SAPC 1.2

3.22.1 Description of Impacts

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

— REST resources on node level:

  • Operator Specific Information

  • Shared Dataplans

— Aggregable Dataplans for Fair Usage Policies

— Default Dataplan priority

3.22.2 Interface

No impact

3.22.3 Operation

No impact

3.22.4 Other Impacts

User experience is improved as follows:

— Maximum value checks are provided for QoS profiles

— Enhanced operator specific information and traffic identifiers handling for subscriber creation procedure

3.23 Virtualization and Cloud Improvements in SAPC 1.2

Introduced in: SAPC 1.2

3.23.1 Description of Impacts

The following functions are supported:

— Workflows for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) in VMware deployments with vCloud Director.

— Additional workflows for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) with HEAT.

— VM Evacuation is supported for new SAPC deployments in:

  • VMWare (vSphere HA): Supported for all VM types (System Controllers, Traffic Processors and Virtual Router VMs).

  • OpenStack based NFVIs: Supported for Traffic Processors and Virtual Routers VMs.

— The OVFgen and HOTgen tools for deployment package generation are combined in one single tool, the `SAPC_descriptor_generator`. For more information on deployment packages, see the SAPC VNF Descriptor Generator Tool.

— The `SAPC_scaleout.py`, `SAPC_scalein.py`, and `SAPC_decommission.py` scripts used during the scale and decommission procedures are replaced by the `SAPC_orchestrator` tool. For more information, see SAPC VNF Decommissioning Instruction for OpenStack, Configure Scale-Out, and Configure Graceful Scale-In documents.

3.23.2 Interface

Not applicable

3.23.3 Operation

No impact

3.24 Diameter Stack Enhancements in SAPC 1.2

Introduced in: SAPC 1.2

3.24.1 Description of Impacts

Due to this feature, operational enhancements are introduced on the Diameter stack.

3.24.2 Interface

No impact

3.24.3 Operation

The SAPC provides:

— A wide set of Performance Management (PM) measurements on the Diameter Stack function

— A CLI tool (DiaDictManager) for the Diameter stack dictionary management

The C-Diameter 1.2 enhancement modifies the mapping of the following AVPs based on priority:

— `Destination-Host`

— `Destination-Realm (optional)`

— `Origin-Host`

— `Origin-Realm (optional)`

For further details regarding the C-Diameter routing change, refer to Configuration Guide for Diameter.

3.25 Default Dataplan Priority

Introduced in: SAPC 1.2

3.25.1 Description of Impacts

Dataplan management is enhanced by adding a default priority attribute at dataplan level.

3.25.2 Interface

Not applicable.

3.25.3 Operation

— New optional parameter `defaultPriority` is added to the dataplan REST API resource.

3.26 Session Context Exposure

Introduced in: SAPC 1.2

3.26.1 Description of Impacts

The Session Context Exposure enables to store ongoing and closed IP-CAN sessions into the external or internal database and access them by REST API.

3.26.2 Capacity and Performance

There are some significant impacts for storing the session context.

— For SAPC deployment with the external database:

- CCR/CCA response time is impacted due to extra CPU time to encode and decode OngoingSession and ClosedSession attributes.
- The LDAP TPS between SAPC and CUDB is impacted because the LDAP request response time between SAPC and CUDB is longer than before.

— For SAPC deployment with the internal database:

- The dimensioning of SAPC is impacted due to extra memory for storing the closed sessions.
- The efficiency of session clean-up is impacted because the extra CPU time is needed at the session termination.

CUDB performance and dimensioning are impacted because more memories and CPU time are consumed for storing session context.

3.26.3 Interface

Analytics REST interface is used for fetching subscriber state and information.

3.26.4 Operation

Added a new EDS for the session context.

Added a new class `SessionInfoPublicationConfig` in the MOM, and two new attributes in it:

— `enableSessionInfoPublication`, to enable or disable this function.

— `durationSessionInfoPublication`, to indicate the maximum storage time of the closed session.

3.27 REST API to Translate Session IP Address to IMSI

Introduced in: SAPC 1.2

3.27.1 Description of Impacts

The REST API to translate session IP address to IMSI function enables the operator to query an IMSI list of ongoing sessions by IP address, APN (if available) and PCEF (if available).

3.27.2 Capacity and Performance

No impact

3.27.3 Interface

Analytics REST interface is used for retrieving an IMSI list from ongoing sessions matching the input criteria.

3.27.4 Operation

No impact

3.28 Use Local Time and Ignore Received 3GPP-MS-TimeZone AVP

Introduced in: SAPC 1.3

3.28.1 Description of Impacts

The SAPC can be configured by means of a configuration parameter to use local time and ignore the `3GPP-MS-TimeZone` AVP received from the Enforcement Function, for group activation or deactivation time, the usage accumulator lifetime, and ToD based policies.

3.28.2 Capacity and Performance

No impact

3.28.3 Interface

No impact

3.28.4 Operation

Added a new parameter `enableMsTimeZone` to the `AppConfig` class in the MOM to enable or disable this function.

3.29 Virtualization and Cloud Improvements in SAPC 1.3

Introduced in: SAPC 1.3

3.29.1 Description of Impacts

The following functions are supported:

- VMware Paravirtual Small Computer System Interface (SCSI) controller type for new SAPC deployments in VMware environment
- Use of the same disk image for both System Controllers in new SAPC deployments in OpenStack environment
- Live migration for the SAPC in VMware environment (vSphere vMotion)
- Dynamic MAC addresses (configuration of MAC addresses assigned by the VIM) for new SAPC deployments in OpenStack using HOT Descriptors
- The customization of MAC addresses during deployment can be done either using the Adapt Cluster Tool (see the *Interface* section in Adapt Cluster Tool) or dynamically retrieving the MAC addresses from the virtual infrastructure.

  Both procedures are supported for VMware and OpenStack (using HOT descriptors). For OpenStack deployment using OVF only MAC addresses customization through the Adapt Cluster Tool is supported.
- Port security configuration for new SAPC deployments in CEE. The activation of port security is supported only for CEE deployments with non-SDN configuration and IPv4
- Use of HOT descriptor files to deploy SAPC from ECM NFVO
- Compact deployments through VNF Lifecycle Manager workflows are deprecated

— Improvements for the VNF Lifecycle Manager workflows in OpenStack environments

  • The `pmEnabled` parameter is set to true by the Instantiation workflow

3.29.2 Capacity and performance

No impact

3.29.3 Interface

Not impact

3.29.4 Operation

No impact

3.30 Policy Studio Improvements in SAPC 1.3

Introduced in: SAPC 1.3

3.30.1 Description of Impacts

The following functions are supported:

— Import/Export of one individual Subscriber

— Volte policy tags related to the following features:

  • IMS restoration

  • Flexible ARP mapping

  • Netloc for untrusted Wlan

  • Group priority check based on accumulation data

  • Rx request type

— Multimedia Priority Services

— Notification of Signalling Path Status

— 5G QCI values support in Content QoS profile

3.30.2 Interface

No impact

3.30.3 Operation

No impact

3.30.4 Other Impacts

User experience is improved as follows:

— Enhanced collection handling

3.31 Security Management Improvements in SAPC 1.3

Introduced in: SAPC 1.3

3.31.1 Description of Impacts

The SAPC creates and manages the following roles in the COM domain:

— SuperUser

— SapcProvisioningAdministrator

— SapcSystemReadOnly

For more information, see System Administrator Guide and SAPC Security User Guide.

3.31.2 Interface

Users must be authorized to access the REST interfaces. The authorization on REST API is mapped with the roles and rules defined in COM.

3.31.3 Operation

No impact

3.32 CNOM Support Improvements in SAPC 1.3

Introduced in: SAPC 1.3

3.32.1 Description of Impacts

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

— Traffic Analysis

3.32.2 Interface

No impact

3.32.3 Operation

No impact

3.33 Session Handler Tool

Introduced in: SAPC 1.3

3.33.1 Description of Impacts

The Session Handler tool enables the operator to access relevant information regarding the sessions of a specific subscriber, for all the applicable protocols. The tool also allows the termination of retrieved sessions for the Gx and Rx protocols.

3.33.2 Interface

When the tool is used to terminate Gx or Rx sessions, it sends the corresponding protocol termination messages to the Gx or Rx interfaces respectively, and also to the session interfaces when applicable (Sy and Sd).

3.33.3 Operation

The operator is expected to do all the session handler tool activities using a CLI command.

3.34 Error Handling of PCC Rule Installation in SAPC 1.4

Introduced in: SAPC 1.4

3.34.1 Description of Impacts

The notification of inactive service data flows to the AF is improved providing the PCC rule installation error handling when connectivity issues occur towards the PCEF.

3.34.2 Interface

— Gx: Added the DIAMETER_UNABLE_TO_DELIVER (3002) value in the `Result-Code` AVP in RAA messages.

— Rx: Supports RAR and ASR messages to notify the AF about PCC rule installation failure due to connectivity issues if the AF subscribed to the INDICATION_OF_RELEASE_OF_BEARER or INDICATION_OF_FAILED_RESOURCES_ALLOCATION events.

3.34.3 Operation

No impact

3.35 Security Management Improvements in SAPC 1.4

Introduced in: SAPC 1.4

3.35.1 Description of Impacts

In addition to the SuperUser, SapcProvisioningAdministrator, and SapcSystemReadOnly roles, the SAPC also supports the following default roles:

— LocalAuthenticationAdministrator

— SapcSystemAdministrator

— SapcSystemSecurityAdministrator

— SapcOperator

— SapcTroubleshooter

The administrators with the SuperUser and SapcSystemSecurityAdministrator roles can create new administrators with custom roles and custom rules.

3.35.2 Interface

No impact

3.35.3 Operation

No impact

3.36 Policy Studio Improvements in SAPC 1.4

Introduced in: SAPC 1.4

3.36.1 Description of Impacts

The following functions are supported:

— Quota Rollover

— Stackable Dataplans

3.36.2 Interface

No impact

3.36.3 Operation

No impact

3.36.4 Other Impacts

User experience is improved as follows:

— Condition Builder advanced manual editor

A new deployment mechanism is provided as a Virtual Machine, with all the software needed by Policy Studio already installed, suitable to be deployed in Cloud environments.

3.37 Optimized Query towards CUDB

Introduced In: SAPC 1.4

3.37.1 Description of Impacts

The SAPC makes an optimized query to retrieve the subscriber profile using the traffic identity as key.

3.37.2 Capacity and Performance

The CCR and CCA response time is improved as the SAPC is able to retrieve the subscriber profile by using one simple query with the traffic identity as key.

The CUDB performance and dimensioning are improved because the SAPC makes one simple query instead of two queries when the traffic identity is different from the administrative identity.

3.37.3 Interface

No impact.

3.37.4 Operation

The following EDSs have been updated:

- `SubscriberIdentity`
- `Subscriber`
- `GroupsToSubscriber`
- `AccumulatedUsage`
- `SessionInfo`

Refer to Integration in User Data Consolidation to configure the new optimized query.

3.38 Virtualization and Cloud Improvements in SAPC 1.4

Introduced in: SAPC 1.4

3.38.1 Description of Impacts

The following functions are supported:

- The possible values for the `target_cloud_system` in the VNF Descriptor Generator Tool have been updated. For details on the particular values available, refer to SAPC VNF Descriptor Generator Tool
- The port security configuration supported only for CEE deployments with non-SDN configuration and IPv4 is now also supported with IPv6 deployments
- The Manual Onboarding, Instantiation, and Termination workflows have been added for lifecycle management through the Virtual Network Function

Life Cycle Manager (VNF-LCM) in OpenStack environments with ECM as NFVO (Or-vnfm support).

— The Openstack environment wokflow have been improved:

  • The drop-down list to select the stack to terminate only shows the SAPC stacks.

  • The SSH key-pair for VNF-LCM workflows is used for all the VNFs managed by this VNF-LCM.

— By default, IPvlan is activated in all deployments.

3.38.2 Capacity and Performance

3.38.3 Interface

No impact

3.38.4 Operation

No impact

3.39 Collision Detection Control

Introduced in: SAPC 1.5

3.39.1 Description of Impacts

The introduction of the CDC mechanism permits to offer the Shared Data Plans feature with an external database. The support of the Collision Detection Control (CDC) mechanism allows the SAPC to store the sharedDataPlan accumulation data in an external database, to detect collisions in write operations for accumulators and to retry the accumulation in case of a collision.

3.39.2 Capacity and Performance

In case of collision during writing operation, the SAPC reattempts the write operation, so the response time for the incoming traffic served by the SAPC is increased accordingly.

If the Shared Data Plan is stored in an external database, the SAPC makes an additional query to retrieve the Shared Data Plan profile and also makes an additional writing operation for its accumulator.

3.39.3 Interface

No impact

3.39.4 Operation

CDC attribute added in the following EDS:

— AccumulatedUsage

Updated the available EDSs for the Shared Data Plan:

— SharedDataplan

— GroupsToSharedDataPlan

— AccumulatedUsageSharedDataPlan

Impacts on the logging events due to the CDC mechanism support:

— Received usage: Added new reason (`value '3'`).

— The following event log is added: `Update Accumulated Usage Failed`

The following measurement is added:

— `ldapCollisionModifyResponses`

3.40 SAPC Session Collector Tool

Introduced in: SAPC 1.5

3.40.1 Description of Impacts

The SAPC Session Collector tool enables the operator to collect data from dynamic Persistent Object Types (POTs) for session backup. For more information, see SAPC Troubleshooting Guide.

3.40.2 Interface

No impact

3.40.3 Operation

No impact

3.41 Policy Studio Improvements in SAPC 1.5.1

Introduced in: SAPC 1.5.1

3.41.1 Description of Impacts

The following functions are supported:

— Refillable Dataplans

— Access Network Charging Identifier (AN-CID)

3.41.2 Interface

No impact

3.41.3 Operation

No impact

3.41.4 Other Impacts

User experience is improved as follows:

— Export all Rules and Export all Rules Spaces are available when exporting objects from a SAPC

— Export All, allows to export all objects in a SAPC with a single click

— Import All, allows to import all objects from a file by overwriting the existing objects, with a single click

— Notification Builder to create notifications according to the Rules Notifications language

3.42 Virtualization and Cloud Improvements in SAPC 1.5.1

Introduced in: SAPC 1.5.1

3.42.1 Description of Impacts

The following functions are supported:

— Manual Scale-Out, Scale-In and auto Scale-Out Workflows have been added for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments with EO as NFVO.

3.42.2 Capacity and Performance

No impact

3.42.3 Interface

No impact

3.42.4 Operation

No impact

3.43 Deployment Improvements in SAPC 1.6.0

Introduced in: SAPC 1.6.0

3.43.1 Description of Impacts

The following functions are supported:

— Previous limitation for initial deployments with just 2 payload nodes is removed. The SAPC can be initially deployed with the total number of payloads required by the customer (at least 2, maximum 45 for VNF deployments, and 34 for PNF deployments).

Note: As in previous SAPC releases, the PLs created during the initial deployment cannot be scaled-in later.

— Watchdog device default configuration can be modified during deployment. Refer to related parameters in Adapt Cluster Tool.

3.43.2 Capacity and Performance

Deployment time for small sizes (2+2) is slightly increased. Deployment time for medium/large sizes is improved. Additional information on instantiation times can be found in the Dimensioning Guidelines.

3.43.3 Interface

No impact

3.43.4 Operation

The number of PLs of initial deployment can be configured to the total number of payloads required by the customer. Check Deployment Instructions for both VNF and PNF deployments for further steps.

To allow the number of initial PLs to be configurable, the IP address for the NFS server has been modified from the previous .100 address on the Internal Network to .243.

3.44 Global Scope Subscriber Group

Introduced in: SAPC 1.6.0

3.44.1 Description of Impacts

The SAPC supports global scope subscriber groups. Global scope subscriber groups are common subscriber groups provisioned with the global scope attribute set to `true` value. The global scope subscriber groups apply to all the SAPC subscribers.

3.44.2 Capacity and Performance

No impact

3.44.3 Interface

The optional `globalScope` attribute is added to the dataplan REST API resource.

3.44.4 Operation

No impact

3.45 Policy Studio Improvements in SAPC 1.6.0

Introduced in: SAPC 1.6.0

3.45.1 Description of Impacts

The following functions are supported:

— Global scope dataplans

— All SAPC policy tags are available in the condition builder

— All SAPC formula expressions are available in the condition builder

— CPI online documentation of tags and functions are available in the condition builder

3.45.2 Interface

No impact

3.45.3 Operation

No impact

3.45.4 Other Impacts

The user experience is improved as follows:

— To improve security, the connections to SAPC nodes can be configured as **Production Nodes**, to prevent accidental modifications to any production node.

— The edition and visualization of the dataplans are improved with an easier way to manage the usage limits.

— The exported JSON files are sorted in a consistent order so that consecutive export files can be easily compared with any standard diff tools.

3.46 Provisioning REST API Improvements in SAPC 1.6.0

Introduced in: SAPC 1.6.0

3.46.1 Description of Impacts

Provisioning REST API is enhanced to support filter on partially REST resources to retrieve the expected resource information.

3.46.2 Capacity and Performance

If the REST resources, such as subscribers and presence-report-area, contain a large amount of data, the CPU load increases significantly. Therefore, it is recommended to schedule the searching requests at an off-peak time.

3.46.3 Interface

No impact

3.46.4 Operation

This function supports search capabilities and queries. For more information, see the Provisioning REST API.

3.47 Logging Improvements in SAPC 1.6.0

Introduced in: SAPC 1.6

3.47.1 Description of Impacts

New informational logs from SAPC 16B were added. For more information see Logging Events.

Support of real-time configuration for each specific log.

— The SAPC provides the capability of enabling or disabling each specific log for reporting purposes. It also ensures the ability of modifying the assigned severity of a specific log by configuration.

Export logs to external system.

— This feature enables the operator to export logs out of the node using SFTP endpoints. This feature can be useful for network or system administrators. For more information see Logging Events.

3.47.2 Capacity and Performance

The logging system is changed to use `syslog` instead of the Core Middleware (CoreMW) logging system, which is based on `saflog`. It improves the maximum number of logging events per second (LPS).

In a configuration of 10 PLs, the number of dropped logging events is expected to be less than 2% when LPS reaches 110000 LPS. The percentage of dropped logging events may increase at a higher rate of LPS.

Warning!

Logging Level 6 impacts the CPU load and NFS speed in SCs and even in the PLs. The performance impact depends on the HW and CPU assignation in the SCs and on the number of PLs and the traffic model. As an example:

— In a BSP with 3 subracks containing 2 SCs +34 PLs, the measured impact is around a 10% increase in the CPU load of the Active SC.

— In a VNF deployment with 2 vCPUs per SC and 16 vCPUs per PL (10 PLs), the measured impact is around a 30% increase in CPU load of the Active SC.

The default value of the Logging Level is 3.

3.47.3 Interface

No impact

3.47.4 Operation

The path where the logs are stored changed to `/cluster/storage/no-backup/coremw/var/log/syslog/sapc`.

For more information, refer to the *Reported Log Files* table in Logging Events.

3.48 Manage Diameter Peer Status / Diameter Connections

Introduced in: SAPC 1.6.0

3.48.1 Description of Impacts

The SAPC provides Northbound Interface (NBI) based peer and diameter link monitoring and management:

— Capability to monitor peer status. Shows peer related information.

— Capability to monitor diameter peer connections.

— Capability to close diameter peer connections with configurable Disconnect-Cause AVP sent through Disconnect Peer Request (DPR) message.

— Capability to manually enable or disable diameter connections.

New alarms are introduced in C-Diameter. These new alarms are linked to the Otpdia MOM:

— When communication is lost with a peer

— When own node is disabled by the operator

— When peer node is disabled by the operator

— When link is down (indicating a connection level failure)

— When link is congested, for congestion handling in general (threshold on C-Diameter counters)

3.48.2 Capacity and Performance

No impact

3.48.3 Interface

Otpdia model is now exposed through NBI. Operator can use COM (netconf / cliss) to configure diameter parameters and to trigger some actions.

Note: Diameter configuration through NBI is stricter in its validity checks and it is possible that adding new configurations reusing previous ones may report errors. Proper configuration examples are included in Configuration Guide for Diameter document.

3.48.4 Operation

No impact

3.49 VNF-LCM Workflows Improvements in SAPC 1.6

Introduced in: SAPC 1.6

3.49.1 Description of Impacts

The following functions are supported:

— The Auto Scale-In Workflow has been added for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments with and without EO as NFVO, and for vCD environments.

— The alarm which triggers the Auto Scale-Out Workflow has been updated to use the new SRM Alarm System Resources High Usage.

— The wrapper file for VNF-LCM Workflows in OpenStack with EO as NFVO has been improved to permit the definition of external network IDs during Instantiation.

3.49.2 Capacity and Performance

No impact

3.49.3 Interface

No impact

3.49.4 Operation

The following alarms are added:

— SRM Alarm System Resources High Usage

— SRM Alarm System Resources Low Usage

3.50 Policy Studio Improvements in SAPC 1.7.0

Introduced in: SAPC 1.7.0

3.50.1 Description of Impacts

User experience is improved as follows:

— Home page redesign:

  • All types of objects are displayed on the home page, with their statistics

  • A table with the most recently modified objects of any type is displayed

  • Global search is enabled, allowing the user to search for any object type from the home page.

— Cross references, allowing the user to find the referenced subject in all relevant subjects. For instance, the user can find the referenced policy in specific Dataplans.

— Dataplan on one page, showing all information related to a Dataplan in the same page, avoiding to find nested references through multiple pages.

3.50.2 Interface

No impact

3.50.3 Operation

No impact

3.50.4 Other Impacts

No impact

3.51 Network License Server

Introduced in: SAPC 1.7.0

3.51.1 Description of Impacts

The SAPC supports the Network License Server (NeLS) in both VNF and PNF deployments. The operator can select the ELIM or the NeLS deployment mode at installation time by modifying the corresponding parameters in `adapt_cluster.cfg` file.

The SAPC supports License Manager (LM) operating in Integration Unlock mode for 21 days.

Note: For newly deployed SAPC systems, the LM is in Integration Unlock (IU) mode for 21 days. All the licenses are granted in IU mode. License checks and license control is managed by the SAPC. If the operators do not request all licenses for the SAPC before the IU mode period ends, alarms are raised to indicate the licenses which are not requested. These licenses are not granted after the IU mode period. When the IU mode period ends, the LM starts to operate in Normal mode, and the alarms are cleared. This does not appear in the upgrade process.

The SAPC supports migration from an ELIM deployment to a NeLS deployment by running a switch process after the SAPC is upgraded to SAPC 1.7.0 or later versions. After switching, the SAPC stops using node-based licensing and connects to the configured NeLS server to request the use of the licenses for features and capacity. Before switching from ELIM to NELS, make sure the LKF is installed in the NELS. The LKF has to have the capacity equal to the sum of the capacities in the LKFs for all nodes in the network. In case that Geographical Redundancy is deployed, the ordered capacity must be double the amount of IP sessions. The ELIM to NeLS switch is unidirectional.

From this release, CBA License Manager 6.8 is adopted, and only the Symantec based certificates are supported to set up the connection with the NeLS.

3.51.2 Capacity and Performance

No impact

3.51.3 Interface

No impact

3.51.4 Operation

The following parameters are added in the adapt_cluster.cfg file:

— LKF_FORMAT

— NELS_HOST

— NELS_PORT

For more information, see Adapt Cluster Tool.

The following Alarms reported on NeLS server are impacted by this function:

— NLM License Not Available

— NLM Capacity Usage Threshold Reached

— NLM License Repository Fault

3.52 Virtualization and Cloud Improvements in SAPC 1.7

Introduced in: SAPC 1.7

3.52.1 Description of Impacts

The following functions are supported:

— The Auto Healing Workflow have been added for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments without EO.

— New Operating Instruction for Manual Healing is provided for VNF deployments in OpenStack.

Note: The Healing operation, both manual or via VNF-LCM workflows, is only supported for new SAPC1.7 deployments or SAPC1.7 deployments coming from an upgrade from SAPC1.6 as the older version.

3.52.2 Capacity and Performance

No impact

3.52.3 Interface

No impact

3.52.4 Operation

No impact

3.53 Security Management Improvements in SAPC 1.8

Introduced in: SAPC 1.8.0

3.53.1 Description of Impacts

The SAPC allows to define user roles with specific access rights for the different REST API end-points (highest REST resources) using custom rules.

For more information, refer to the System Administrator Guide document.

3.53.2 Capacity and Performance

No impact

3.53.3 Interface

No impact

3.53.4 Operation

No impact

3.54 Fair Usage Control for Preconfigured and Dynamic Services

Introduced in: SAPC 1.8.0

3.54.1 Description of Impacts

The SAPC supports Fair Usage Control for preconfigured and dynamic services by associating with the Monitoring Key. The operator can provision Monitoring Keys unconditionally and configure Monitoring Key Selection policies.

3.54.2 Capacity and Performance

No impact

3.54.3 Interface

— Provisioning REST API: added the `contentMonitoringKey` attribute in `/contents/{contentName}/static-qualification`.

— Gx: added `Monitoring-Key` AVP within the `Charging-Rule-Definition` AVP.

3.54.4 Operation

The following policy type is added:

— Monitoring Key.

The following change is done to Logging Events:

— Monitoring-Key is added in the Rule to Install event.

The following change is done for Event-Based Monitoring:

— The value of Monitoring Key is set in the RULE_INSTALLED event.

3.55 Virtualization and Cloud Improvements in SAPC 1.8

Introduced in: SAPC 1.8

3.55.1 Description of Impacts

The following functions are supported:

— For SAPC deployments on OpenStack based NFVIs, the VM Evacuation is supported for all VM types (System Controllers, Traffic Processors and Virtual Router VMs). Refer to the SAPC VNF Descriptor Generator Tool document.

— Scale-in procedure (sapcScaleIn tool) is improved to minimize the traffic loss by modifying the Diameter expiration timeout during the procedure execution. Once finished, the timeout is set to the previous value.

— The Auto Healing Workflow has been added for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments with EO.

— For External Database configurations, the Adapt Cluster tool requires that the `EDB_VIP` parameter, when configured, is included in the extDB section of the configuration file as described in the Adapt Cluster Tool document.

3.55.2 Capacity and Performance

No impact.

3.55.3 Interface

No impact.

3.55.4 Operation

No impact

3.56 Policy Studio Improvements in SAPC 1.8.0

Introduced in: SAPC 1.8.0

3.56.1 Description of Impacts

The following function is supported:

— Reference filters in Subscribers, which can find subscribers that are using a particular shared dataplan.

3.56.2 Interface

No impact

3.56.3 Operation

No impact

3.56.4 Other Impacts

No impact

3.57 Default PCEF

Introduced in SAPC 1.8.0

3.57.1 Description of Impacts

The SAPC supports the definition of the Default PCEF to avoid adding each PCEF configuration individually. The Default PCEF is compatible with particular PCEF configuration even cluster PCEF configuration.

For PCEFs using the Default PCEF, the PCEF peer identifier reported as Measured Object Instance is the `Origin-Host` AVP.

Refer to the Configuration Guide for Access and Charging Control (Gx) and the Configuration Guide for Dynamic Policy Control (Rx) for details.

3.57.2 Capacity and Performance

No impact

3.57.3 Interface

— Gx

- When the SAPC has a Default PCEF configured, incoming connections from any unknown PCEF are accepted and the configuration of the Default PCEF is applied to it. After that, the unknown PCEF interacts as any other PCEF configured individually.

3.57.4 Operation

To add a Default PCEF in the SAPC, the operator has to create a `DiameterNode` with the `diameterNodeId` equal to the case sensitive value Default.

3.58 UE Trace Tool Improvements for SAPC 1.9

Introduced in: SAPC 1.9

3.58.1 Description of Impacts

The UE Trace Tool enables the operator to collect Sd incoming and outgoing messages for a set of User Equipments (UEs) in a similar way as it is done for Rx and Gx.

The configuration of Gx, Rx, Sd listening ports in cfg file is not needed anymore. They are taken directly from SAPC COM configuration.

3.58.2 Capacity and Performance

No impact

3.58.3 Interface

In the Sd interface the SAPC is able to:

- Activate or deactivate incoming and outgoing UE traces for a user indicated by the `subscriberId` AVP
- Show UE trace sessions that are being traced
- Collect messages filtered for subscriber ID in MSISDN or IMSI format
- Schedule trace sessions
- See a trace in real-time using the UE Trace viewer
- Generate an `xml` and a `pcap` file containing messages from all active UE tracing sessions

3.58.4 Operation

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

3.59 Gx Rel8 support

Introduced in: SAPC 1.8.0 EP1

3.59.1 Description of Impacts

The SAPC supports interoperability with PCEFs handling Gx Rel8.

3.59.2 Interface

SAPC provides support for Gx Rel8:

- `Flow-Description` AVP uplink (direction 'in') inside `Flow-Information` is supported.
- `Flow-Direction` AVP is not supported. `Event-Triggers` related to each version is used.
- Corresponding Gx Rel 8 values for `Event-Triggers` are used.

3.59.3 Operation

Existing `gxRel910rLowerCompatibility` configuration parameter is also used to enable the support for interoperability with PCEFs handling Gx Rel8.

3.60 Subscriber Session Cleanup

Introduced in: SAPC 1.9

3.60.1 Description of Impacts

The SAPC provides an automatic cleanup mechanism to remove the obsolete Gx sessions. A session is treated as obsolete when new CCR-I is received with the same Subscriber Id, same APN, same Traffic Id and different IP.

3.60.2 Interface

No impact

3.60.3 Operation

Added a new class `SubscriberSessionCleanupConfig` in the MOM, and two new attributes in it:

— `enabledCleanup`, to enable or disable this function.

— `checkForSessionAlive`, to indicate if the SAPC sends an RAR message to the PCEF to check session is alive or not.

3.61 Virtualization and Cloud Improvements in SAPC 1.9

Introduced in: SAPC 1.9

3.61.1 Description of Impacts

— VNF deployments including Virtual Routers are deprecated. New deployments with this configuration are not allowed. For existing deployments, a procedure based on the upgrade by replacement method is provided to migrate to new deployments without Virtual Routers.

— A new alarm is provided to report the loss of communication with a distributed storage.

3.61.2 Capacity and Performance

No impact.

3.61.3 Interface

No impact.

3.61.4 Operation

No impact.

3.62 VNF-LCM Workflows Improvements in SAPC 1.9

Introduced in: SAPC 1.9

3.62.1 Description of Impacts

The following functions are supported:

— The Upgrade Workflow has been added for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments without EO.

— Keystone v3 is supported in OpenStack deployments.

3.62.2 Capacity and Performance

No impact.

3.62.3 Interface

No impact.

3.62.4 Operation

No impact.

3.63 Network License Server Improvements in SAPC 1.9

Introduced in: SAPC 1.9.0

3.63.1 Description of Impacts

CBA License Manager 6.10 is adopted: The Symantec-based certificates can still be used, and for NeLS version 2.5 or upward, EPPKI certificate can also be used.

For more information, see SAPC License Management.

3.63.2 Capacity and Performance

No impact

3.63.3 Interface

No impact

3.63.4 Operation

No impact

3.64 UE Trace Tool for Sy

Introduced in: SAPC 1.10

3.64.1 Description of Impacts

Incoming and outgoing messages for a set of User Equipments (UEs) can be collected through the Sy and eSy interfaces in the same way as for Rx, Gx and Sd interfaces.

3.64.2 Capacity and Performance

No impact

3.64.3 Interface

Using the Sy interface, 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 Sy and eSy messages filtered for subscriber ID in MSISDN or IMSI format
- Schedules trace sessions
- Displays a trace in real-time using the UE Trace viewer

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

3.64.4 Operation

All tracing activities must be completed using CLI commands.

3.65 Soft-Limit License Behavior Improvements in SAPC 1.10

Introduced in: SAPC 1.10

3.65.1 Description of Impacts

The soft-lock principle (alarms and reports are issued but the node service is not restricted) is supported in the following scenarios:

— When the license keys are expired or to be active in the future

— When capacity license limit is surpassed

— When abnormal situations, as loss of communication towards the license server, file corruption, ... (in this case the node runs in the AU mode)

This new behavior applies to both NeLS and ELIM deployment modes.

For more information, see SAPC License Management.

3.65.2 Capacity and Performance

No impact

3.65.3 Interface

No impact

3.65.4 Operation

No impact

3.66 Policy Studio Improvements in SAPC 1.10

Introduced in: SAPC 1.10

3.66.1 Description of Impacts

— Support for Dynamic Subscriber Update

3.66.2 Capacity and Performance

No impact

3.66.3 Interface

No impact

3.66.4 Operation

No impact

3.67 HTTP/2 Connection

Introduced in: SAPC 1.10.0 with Limited Availability, SAPC 1.11.0 with General Availability

3.67.1 Description of Impacts

HTTP/2 defines multiplexing on a single connection, which allows multiple requests sent in parallel, without the need to wait for response of precedent requests.

Note: HTTP 1.1 and HTTP 1.0 traffic is not supported.

— When the SAPC PCF acts as a client, the HTTP/2 connection provides the following functions:

  - Long-lived connection
  - Configurable connection numbers
  - Reset or re-establish connection on Stream-ID exhaustion
  - Reconnect on failure connection
  - Load balance on connections (round robin, priority, weighted)

— When the SAPC PCF acts as a server, the traffic to the SAPC PCF is distributed evenly to PLs.

The HTTP/2 Connection supports the following two ways to deploy the redundancy model:

— NWay redundancy model

— 2N redundancy model

Note: Depending on the traffic mode and number of PLs, the traffic of the PL node on that the HTTP/2 proxy is deployed has the heaviest load, and may become overloaded.

For more information, see HTTP/2 Connection Management.

3.67.2 Interface

No impact

3.67.3 Operation

Class `PcfForwardProxy` is added in MOM.

3.68 Session Management Policy Control

Introduced in: SAPC 1.10.0 with Limited Availability, SAPC 1.11.0 with General Availability

3.68.1 Description of Impacts

The Session Management (SM) policy control function is supported by the SAPC PCF through the N7 interface. The SM policy control adheres to the policy control framework of the 5GC architecture and its defined Npcf service based interface.

The SAPC PCF provides the following functions:

— SM policy association establishment, modification, and termination.

— QoS Control

  The SAPC PCF supports the Session QoS control and QoS control to PCC rules.

— Gating Control

  Gating Control is a user plane function, enabling or disabling the forwarding of data packets from service data flows.

— Policy control request trigger selection

  Policy control request trigger is the condition when the SMF interacts again with the SAPC PCF for further policy decision of a PDU session.

— Dynamic Group Selection

  Dynamic selection of subscriber groups is performed using group selection policies including operator configured conditions.

— Usage Monitoring Control

  The Usage Monitoring Control enables the SAPC PCF to control the accumulated volume assumed at service level. Usage limits can be only applied to volume.

  The SAPC PCF only supports Usage Monitoring Profiles at subscriber group level and does not support shared subscriber plans.

  The SAPC PCF supports the accumulation of usage information only in the internal database. For subscribers capable in both 4G and 5G network, the SAPC PCF does not support the usage accumulators stored in the separated databases.

For more information, refer to Access and Charging Control (N7).

3.68.2 Capacity and Performance

The capacity license of the SAPC is updated to control PDU sessions over N7 interface. Therefore, the active PDU sessions created through N7 interface are counted in total number of active mobile sessions.

3.68.3 Interface

— N7—The SAPC PCF supports messages exchanged for the following service operations over N7 interface:

  • Npcf_SMPolicyControl_Create

  • Npcf_SMPolicyControl_UpdateNotify for session modification

  • Npcf_SMPolicyControl_Update

  • Npcf_SMPolicyControl_Delete

  For detailed messages supported, see N7 Interface Description.

— Provisioning REST API—Added the following attributes under the /contents/{contentName} URI:

  • `flowStatus`: status of the flow.

  • `defQosFlowIndication`: indicates whether the dynamic PCC rule always has its binding with the QoS flow associated with the default QoS rule.

3.68.4 Operation

The following alarms are added:

— Policy Control, Number of Npcf_SMPolicyControl Policy Request Failure Reached

— Policy Control, Number of PCF Initiated Npcf_SMPolicyControl Update Notify Failure Reached

The following Key Performance Indicators are added:

— SM Policy Control Create Failure Ratio

— SM Policy Control Update Failure Ratio

— SM Policy Control UpdateNotify Failure Ratio

— SM Policy Control Transactions per Second

The following NpcfSm protocol measures are added:

— NpcfSmCreateFailed

— NpcfSmCreateSuccess

— NpcfSmDeleteFailed

— NpcfSmDeleteSuccess

— NpcfSmRespFailed

— NpcfSmUpdateFailed

— NpcfSmUpdateNotifyFailed

— NpcfSmUpdateNotifyRequests

— NpcfSmUpdateNotifySuccess

— NpcfSmUpdateSuccess

— NpcfSmCreateRequests

— NpcfSmUpdateRequests

— NpcfSmDeleteRequests

— NpcfSmUpdateErrorInitialParameters

— NpcfSmUpdateErrorTriggerEvent

— NpcfSmUpdateNotifyFailedPccRuleEvent

— NpcfSmUpdateNotifyFailedPccQosFlowEvent

The following capacity measure is added:

— smfActiveSessions

The mobileActiveSessions measure is also applicable to the SAPC PCF.

The following Logging Events are supported for the SAPC PCF:

— Incoming Bearer QoS

— Internal Error

— Outgoing Bearer QoS

— Outgoing QoS per Rule

— Protocol Error

— Received Usage

— Reset of Accumulated Usage Data

— Rule Installation Failure

— Rule to Install

— Rule to Remove

— Usage Limit Surpassed

The following policy types are supported for the SAPC PCF:

— Event Triggers Selection

— Bearer QoS Control for Service

— Bearer QoS Control for Bearer

The following policy tags are supported for the SAPC PCF:

— Access policy tags:

  • `AccessData.bearer.accessPoint`

  • `AccessData.bearer.accessType`

  • `AccessData.bearer.eventTriggers`

- `AccessData.bearer.requestType`
- `AccessData.subscriber.id`
- `AccessData.subscriber.imsi`
- `AccessData.subscriber.ueIpAddress`
- `AccessData.subscriber.ueIpv6Prefix`
- `AccessData.subscriber.ueIpAddressType`
- `AccessData.subscriber.locationInfo.routingAreaCode`

— Location policy tags:

- `AccessData.subscriber.locationInfo.cellIdentity`
- `AccessData.subscriber.locationInfo.countryCode`
- `AccessData.subscriber.locationInfo.networkCode`
- `AccessData.subscriber.locationInfo.timezone`

— QoS policy tags:

- `AccessData.requestedQos.classIdentifier`
- `AccessData.requestedQos.mbrUplink(Gx)`
- `AccessData.requestedQos.mbrDownlink(Gx)`
- `AccessData.requestedQos.priorityLevel`

— Subscriber Data policy tags:

- `Subscriber.groups`
- `Subscription.group["groupName"].isActive`
- `Subscription.group["groupName"].isSubscribed`

— Usage Monitoring policy tags:

- `AccessData.subscriber.accumulatedUsage.reportingGroup["tota l"/"reportingGroupName"].current["type"]`
- `AccessData.subscriber.accumulatedUsage.reportingGroup["tota l"/"reportingGroupName"].currentPercentage["type"]`
- `AccessData.subscriber.accumulatedUsage.reportingGroup["tota l"/"reportingGroupName"].isLimitSurpassed["type"]For more information on configuration, see`

- `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].current["type"]`

Class `PcfConfig` is added in MOM.

Fore more information, refer to Configuration Guide for Access and Charging Control (N7).

3.69 Dynamic Policy Control (Rx) for SAPC PCF

Introduced in: SAPC 1.10.0 with Limited Availability, SAPC 1.11.0 with General Availability

3.69.1 Description of Impacts

The SAPC PCF provides the following functionality between the SAPC PCF and the AF:

— Voice Support

  Dynamic policy control is supported to bind the Rx session with the N7 sessions from the SMF. It enables the support of voice for EPS fallback.

— Successful Resources Allocation

  Successful Resources Allocation enables the SAPC PCF to provide a notification to the AF when the resources associated to the corresponding service information are allocated successfully.

— Service Data Flow Deactivation

  When a dynamic PCC rule cannot be installed, activated or enforced at the SMF, the SAPC PCF deactivates the corresponding dynamic service and informs the AF that one or more service data flows have been deactivated. This function enables the AF to react to events in the user plane by sending an AAR command to the SAPC PCF to update the session information or an STR command to terminate the AF session.

— NetLoc

  NetLoc is an optional function. The SAPC PCF negotiates its support during the SMF and the AF session establishment. It enables the SAPC PCF to report (onetime report) the network location information during the AF session establishment, modification, or termination.

For more information, see Dynamic Policy Control (Rx) for SAPC PCF.

3.69.2 Capacity and Performance

No Impact

3.69.3 Interface

No impact

3.69.4 Operation

The following policy type is not applicable to the SAPC PCF:

— Service Charging

The following Application (Rx data) tag is not applicable to the SAPC PCF:

— `AfData.mpsIdentifier`

The following policy tag related to AF signaling path notification is not applicable to the SAPC PCF:

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

3.70 Unified Data Repository

Introduced in: SAPC 1.10.0 with Limited Availability, SAPC 1.11.0 with General Availability

3.70.1 Description of Impacts

The SAPC PCF provides the following functions over the N36 interface:

— Retrieval of policy data.

— Subscription and unsubscription of data change notifications.

— Reception of data change notifications.

— UDR 1+1 deployment

  The SAPC PCF selects a primary UDR for traffic. When the primary UDR becomes unavailable, the SAPC PCF performs failover to the secondary UDR. When the primary UDR becomes available again, the SAPC PCF performs failback.

For more information, see Interaction with UDR.

3.70.2 Capacity and Performance

No Impact

3.70.3 Interface

The SAPC PCF supports messages exchanged for the following service operations over N36 interface:

— Nudr_DataRepository_Query

— Nudr_DataRepository_Subscribe

— Nudr_DataRepository_Notify

— Nudr_DataRepository_UnSubscribe

For detailed messages supported, see N36 Interface Description.

3.70.4 Operation

The following changes are done to MOM:

— Added class `PcfPeerNodes` to configure the UDR in the SAPC PCF.

— Added the pcfPriority(integer) and pcfLocality(String) attributes under class PcfAppConfig.

— Class DiscoveredPeerNode can be loaded from NRF.

The following alarms are added:

— Policy Control, Connection to UDR Failed for SM Policy Control

— Policy Control, Failover Caused by Failure on UDR Connection for SM Policy Control

3.71 Network Repository Function

Introduced in: SAPC 1.10.0 with Limited Availability, SAPC 1.11.0 with General Availability

3.71.1 Description of Impacts

The SAPC PCF supports the following functions over the Nnrf interface:

— The SAPC PCF registers, updates or deregisters its profile in the Network Repository Function (NRF).

— The SAPC PCF discovers the Unified Data Repository (UDR) by querying the NRF.

— The SAPC PCF subscribes the notification of UDR when registering and updating in the NRF, and unsubscribes the notification of UDR when deregistering in the NRF.

For more information, see Interaction with NRF.

3.71.2 Capacity and Performance

No Impact

3.71.3 Interface

The SAPC PCF supports messages exchanged for the following service operations over Nnrf interface:

— Nnrf_NFManagement_NFRegister

— Nnrf_NFManagement_NFUpdate

— Nnrf_NFManagement_NFDeregister

— Nnrf_NFManagement_NFStatusSubscribe

— Nnrf_NFManagement_NFSubscriptionUpdate

— Nnrf_NFManagement_NFStatusNotify

— Nnrf_NFManagement_NFStatusSubscribe

— Nnrf_NFDiscovery_NFDiscover

For detailed messages supported, see Nnrf Interface Description.

3.71.4 Operation

No impact

3.72 Session Cleanup Enhancements in SAPC 1.10.0

Introduced in: SAPC 1.10.0 with Limited Availability, SAPC 1.11.0 with General Availability

3.72.1 Description of Impacts

The SAPC PCF supports the following functions to clean up the N7 session:

— N7 session basic cleanup mechanism:

  • When the SAPC PCF receives an N7 session creation request from a given SMF, the SAPC PCF checks whether a duplicate N7 session exists in the SAPC PCF. Duplicate means the two sessions have the same IP address of the UE, DNN, and the node Id (including the IP address and port) of the SMF.

  • As a consequence of the removal of each N7 session, the AF sessions are removed as it is done when an N7 session is terminated. The SAPC PCF requests the AF to revoke all the identified AF sessions.

— N7 Session Inactivity Cleanup Mechanism

  • The SAPC PCF provides an automatic cleanup mechanism to remove all the N7 sessions. A session is considered inactive or obsolete when no Npcf_SMPolicyControl request is received or no notification sent during a configurable period.

— AF node peer restart

  • The SAPC PCF provides a massive cleanup mechanism to remove all the inactive Rx sessions established towards the restarted AF node peer. Meanwhile, the SAPC PCF notifies the SMF of the N7 session that the Rx session is bound to and sends a notification to reauthorize the session.

  • The deletion of the invalid Rx sessions starts immediately after an AF restart is recognized.

For more information, see Availability and Scalability for SAPC PCF.

3.72.2 Capacity and Performance

No Impact

3.72.3 Interface

No impact

3.72.4 Operation

In MOM, the `checkFor5gSessionAlive` attribute is added under class `PcfAppConfig`.

3.73 Session Handler Tool Enhancements in SAPC 1.10.0

Introduced in: SAPC 1.10.0 with Limited Availability, SAPC 1.11.0 with General Availability

3.73.1 Description of Impacts

Session handler is enhanced to support N7 session for the SAPC PCF. The following changes are made to support N7 session:

— Showing and deleting N7 sessions with their dependent Rx sessions of a subscriber.

— Specifying the session type (N7 or Gx) for the delete operation.

3.73.2 Capacity and Performance

No Impact

3.73.3 Interface

No impact

3.73.4 Operation

Added a new parameter `[--sessionType]` in the syntax of session-handler tool.

3.74 Virtualization and Cloud Improvements in SAPC 1.10

Introduced in: SAPC 1.10

3.74.1 Description of Impacts

— Instantiation and termination for TOSCA deployments are now supported through theVirtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments with 3rd party NFVO. The BCAT tool is provided for CSAR Packages generation including hybrid VNFD (TOSCA+HOT).

— The Upgrade Workflow is compatible with GeoRed deployments for lifecycle management through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments without EO.

3.74.2 Capacity and Performance

No impact

3.74.3 Interface

No impact

3.74.4 Operation

No impact

3.75 Support Update Subscriber OSI by Policies

Introduced in: SAPC 1.10.0

3.75.1 Description of Impacts

The SAPC PCRF supports updating subscriber Operator Specific Information (OSI) to the internal database by policies. This is possible using the new policy type Dynamic Subscriber Profile Update.

For details, see Subscription and Policy Management.

Note: Conflict detection is not supported for OSI update in the internal DB. This may happen when multiple IP-CAN sessions update the OSI simultaneously for the same subscriber, or when a provisioning operation on the OSI is running at the same time as one triggered by traffic.

3.75.2 Capacity and Performance

No impact

3.75.3 Interface

No impact

3.75.4 Operation

The Dynamic Subscriber Profile Update policy type is added.

The `WriteSubscriber` EDTarget is defined in MOM.

The Subscriber Operator-Specific-Info Update logging event is added.

For details, see Configuration Guide for Subscription and Policies.

3.76 Diameter Regulation Mechanism

Introduced in: SAPC 1.10

3.76.1 Description of Impacts

The SAPC includes enhancements in handling Diameter messages under massive traffic overload, as well as in situations where an external database or OCS eventually delays the response for a longer time than usual. As a result, the SAPC achieves a better message latency for incoming messages and less opportunities of having either failed or retried operations. These enhancements are additional to the 'Overload Protection of Priority Services' mechanism and cover following cases

— Handling of messages with a high waiting time to be processed:

  • Adaptability in the discarding of these messages for Sd and Smp protocols (only Gx and Rx protocols included this since the SAPC 1.9 version).

  • Avoid discarding incoming answers to the SAPC outgoing request messages. For example: RAA, or ASA.

— Adding retry policy to failed outgoing messages due to traffic overload.

— Adding detection mechanism to avoid sending answers to incoming requests out of expected time by the C-Diameter configuration. These requests will be answered with a 3004 (Diameter Too Busy) response code.

Refer to *Diameter Regulation Mechanism* in Overload Control Facility Description.

3.76.2 Capacity and Performance

No Impact

3.76.3 Interface

No Impact

3.76.4 Operation

Extra information added to logs related with handling of Diameter messages:

— Include the elapsed time to the Discarded Incoming Message log.

— Include the error code for all the Error Sending logs in all the supported Diameter protocols.

3.77 Minimum Requested Bandwidth Support for Guaranteed Bitrate Calculation

Introduced in: SAPC 1.10 EP2

3.77.1 Description of Impacts

The SAPC supports deriving Authorized Guaranteed Data Rate DL/UL or Extended Authorized Guaranteed Data Rate UL/DL from the `Min-Requested-Bandwidth-UL/DL` AVPs or the `Extended-Min-Requested-Bandwidth-UL/DL` AVPs in the service information in Rx Diameter message.

3.77.2 Capacity and Performance

No impact

3.77.3 Interface

— Rx:

- The following new AVPs are added to the `Media-Component-Description` AVP in AAR messages:
  - `Min-Requested-Bandwidth-DL` (AVP code 534)
  - `Min-Requested-Bandwidth-UL` (AVP code 535)
  - `Extended-Min-Requested-BW-DL` (AVP code 560)
  - `Extended-Min-Requested-BW-UL` (AVP code 561)
- New `Supported-Features` AVP instance with `Feature-List-ID` = 2, to support `Extended-Min-Requested-BW-NR` (bit 2).

3.77.4 Operation

No impact

3.78 Access and Charging Control Functionalities for Session Management Policy Control

Introduced in: SAPC 1.11

3.78.1 Description of Impacts

The following Access and Charging Control functionalities are supported by the SAPC PCF:

— PDU Session Access Control

— Service Access Control

— Service Charging Control

Note: If the SMF supports AF_Charging_Identifier feature, `afChargId` carries the AF Charging Identifier sent from AF node.

If the SMF does not support AF_Charging_Identifier feature, `afChargingIdentifer` carries the AF_Charging Identifier sent from AF nodes. However, if the AF Charging Identifier is not an unsigned integer, the `afChargingIdentifier` is omitted in the PCC rule. This hinders the charging correlation between service level and application level report.

— Subscriber Charging Control

For more information, refer to Access and Charging Control (N7) and Dynamic Policy Control (Rx) for SAPC PCF.

3.78.2 Capacity and Performance

No impact

3.78.3 Interface

— Provisioning REST API: Subscriber Charging Control functionality introduces the following attributes to the charging system profile (`profiles/charging-system/{profileId}` URI):

  — `primaryChfAddress`

  — `secondaryChfAddress`

— N7 interface: new attributes are supported. For more information, refer to N7 Interface Description.

— Rx interface: new AVPs are supported. For more information, refer to Rx Interface Description.

3.78.4 Operation

— New extensions are done to MoM:

- Added `controls` attribute under class `PcfPeerNode`.
- Added the following values to `PccControl` enum:
  - `PDU_SESSION_ACCESS` for PDU Session Access Control
  - `SERVICE_ACCESS_PCF_TOD` and `SERVICE_ACCESS_SMF_TOD` for Service Access Control
- Added `SMF` value in enum `PcfNodeType`.

— New policy types are introduced for Access and Charging Control functionalities for session management policy control.
  - Access related policies
  - Charging related policies

For more information on configuration, refer to Configuration Guide for Access and Charging Control (N7).

3.79 Updating Subscriber OSI by Policies Support for External Database

Introduced in: SAPC 1.11.0

3.79.1 Description of Impacts

The SAPC PCRF is enhanced to support updating subscriber OSI by policies to an external database through the LDAP interface.

For more information, refer to Integration in User Data Consolidation.

3.79.2 Capacity and Performance

No impact

3.79.3 Interface

No impact

3.79.4 Operation

No impact

3.80 Virtualization and Cloud Improvements in SAPC 1.11

Introduced in: SAPC 1.11

3.80.1 Description of Impacts

— Instantiation and termination for TOSCA deployments are supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) in VMware vCloud Director environments with 3rd party NFVO. The BCAT tool is provided for CSAR Packages generation including hybrid VNFD (TOSCA+OVF).

— Manual Scale-Out and Scale-In for TOSCA deployments are supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments with 3rd party NFVO.

— New document, SAPC VNF Deployments Overview contains useful information about the different types of VNF deployments supported by SAPC.

3.80.2 Capacity and Performance

No impact

3.80.3 Interface

No impact

3.80.4 Operation

No impact

3.81 Mutual TLS (mTLS) Authentication Support for SBI

Introduced in: SAPC 1.11.0

3.81.1 Description of Impacts

Mutual TLS (mTLS) Authentication is supported by the SBI to ensure the two-way secure communication over the N7, N36, and Nnrf interface between the SAPC and the peer nodes.

For more information, refer to SAPC Security User Guide.

3.81.2 Capacity and Performance

No impact

3.81.3 Interface

No impact

3.81.4 Operation

The TLS Client Authentication of the SAPC needs to be enabled for each interface. The following attributes are added in class `PcfSecurity` in MOM:

— `enableTLSClientAuthenticationSMF`

— `enableTLSClientAuthenticationUDR`

— `enableTLSClientAuthenticationNRF`

A new instance `NodeCredentialId=sapc-client` is introduced to MO Class `NodeCredential`.

A new instance `TrustCategoryId=sapc-ca` is introduced to MO Class `TrustCategory`.

For more information, refer to HTTP/2 Connection Management.

3.82 SAPC PCF Support of Subscriber Operator Specific Information

Introduced in: SAPC 1.11.0

3.82.1 Description of Impacts

Operator Specific Information (OSI) is operator specific data stored in the UDR.

The SAPC PCF can query and update OSI, and subscribes to changes of it. For more information, refer to Interaction with UDR.

The SAPC PCF updates subscriber OSI to the UDR using Dynamic Subscriber Profile Update policies. For the configuration, refer to Configuration Guide for SAPC PCF Subscription and Policies.

The Query, Update, and Subscribe operations related to OSI can be disabled by the `enableOsiInUdr` attribute under class `pcfAppConfig`.

Note: Conflict detection is not supported for OSI update by traffic in UDR. This may happen when multiple PDU sessions update the OSI simultaneously for the same subscriber.

3.82.2 Capacity and Performance

When the `enableOsiInUdr` attribute is set to `true`, the Query, Update, and Notify operations related to operator specific data have impact to the traffic model.

3.82.3 Interface

The following is done to the N36 interface:

— Nudr_DataRepository_Query Response: added map(OperatorSpecificDataContainer) data type.

— Added PATCH Nudr_DataRepository_Update operation.

— Nudr_DataRepository_Subscribe Request: added the `/nudr-dr/v2/policy-data/ues/{ueId}/operator-specific-data` Uri.

— Nudr_DataRepository_Notify Request: added the `opSpecDataMap` attribute.

— Added OperatorSpecificDataContainer data structure.

3.82.4 Operation

Added the `enableOsiInUdr` attribute under class `pcfAppConfig` in MOM.

Added new output attribute `5g-subscriber-update` to the Dynamic Subscriber Profile Update policy type. For details, refer to Configuration Guide for SAPC PCF Subscription and Policies.

3.83 SM Policy Association Establishment without UE IP Address Support

Introduced in: SAPC 1.12

3.83.1 Description of Impacts

The SAPC PCF supports for the SMF to create an SM policy association establishment without UE IP address. This scenario complies with the PDU Session Establishment defined in *3GPP TS 23.502*. The supported scenario is made up of the following two steps:

— Step 1: Reception of `Npcf_SMPolicyControl_Create` request without IP address

- The SMF initiates an SM Policy establishment procedure for a session. The SAPC PCF receives the `Npcf_SMPolicyControl_Create` request. Neither IPv4 address nor IPv6 prefix is included in the request.
- The session is created in the SAPC PCF and marked as pending.
- The SAPC PCF responds to SMF with supported Policy decision.

— Step 2: Reception of `Npcf_SMPolicyControl_Update` request with IP address

- The SMF initiates an SM Policy modification procedure for the pending session. The SMF provides the IP address/prefix of the UE to the PCF in the `Npcf_SMPolicyControl_Update` request.
- The session in the SAPC PCF is marked as normal.
- The PCF sends an updated Policy Decision of the PDU session to the SMF.

For more information, refer to the Access and Charging Control (N7) document.

3.83.2 Capacity and Performance

No impact

3.83.3 Interface

The SAPC PCF supports the following new optional attributes in the `SmPolicyUpdateContextData` data structure contained in the `Npcf_SMPolicyControl_Update` request sent from the SMF to the SAPC-PCF over the N7 interface:

— ipv4Address

— ipv6AddressPrefix

For the details of the supported messages, refer to the N7 Interface Description document.

3.83.4 Operation

For pending sessions, the following logs show an empty string in the IP address field in the Additional Information:

— Existing IP Session removed

— Rule to Install

— Rule to Remove

3.84 Support of GPSI as Subscriber ID

Introduced in: SAPC 1.12.0

3.84.1 Description of Impacts

GPSI received through N7 interface is supported as subscriber identifier, and it can be selected as such by configuring `subsIdType`. For more information, refer to Configuration Guide for Access and Charging Control (N7).

3.84.2 Interface

Added `gpsi` in the SmPolicyContextData data structure over the N7 interface.

3.84.3 Operation

The `AccessData.subscriber.msisdn` policy tag can be used in policy evaluation for N7 sessions.

The result of `AccessData.subscriber.id` depends on the configuration of `subsIdType`.

3.85 New Parameters in SAPC PCF Registration Profile

Introduced in: SAPC 1.12.0

3.85.1 Description of Impacts

The SAPC PCF supports registering more parameters in the NRF.

3.85.2 Interface

Added the following parameters over the Nnrf Interface:

— In NFProfile data structure: `interPlmnFqdn`, `allowedNfDomains`, `nfProfileChangesSupportInd`, and `servingScope`.

— In NFService data structure: `interPlmnFqdn` and `allowedNfDomains`.

— In PcfInfo data structure: `groupId`, `gpsiRanges`, and `v2xSupportInd`.

3.85.3 Operation

Added new parameters in the SAPC PCF registration profile. See the configuration example in Configuration Guide for Interaction with NRF.

3.86 Enable or Disable NRF Discovery for NFs by Configuration

Introduced in: SAPC 1.12.0

3.86.1 Description of Impacts

SAPC PCF provides a configuration parameter to control whether an NF is discovered via the NRF.

3.86.2 Capacity and Performance

No impact

3.86.3 Interface

No impact

3.86.4 Operation

A new configuration parameter, `enableNrfDiscoveryNfs` is available under the `PccAppConfig` class.

3.86.5 Other Impacts

After maiden installation, the list of `enableNrfDiscoveryNfs` is empty, that means no NFs including UDR are discovered via the NRF. But when the SAPC is upgraded to SAPC 1.12.0 or later versions, the UDR is automatically added into the list of `enableNrfDiscoveryNfs` if there is no local UDR information.

3.87 Precedence Calculation for PCC Rules

Introduced in: SAPC 1.12.0

3.87.1 Description of Impacts

When the SAPC PCF installs a new preconfigured or dynamic PCC rule, the SAPC PCF calculates the precedence value of the PCC rule. The precedence value is an

integer in the range from 0 to 255 (0 reserved for SMF, 70 to 99 reserved for the PCC rules subject to Reflective QoS, and 255 reserved by 3GPP).

The SAPC PCF guarantees all PCC rules within a PDU session have different precedence values.

For more information, refer to Access and Charging Control (N7).

3.87.2 Interface

No impact

3.87.3 Operation

The precedence configuration for preconfigured PCC rules through provisioning REST API for 5G services is the same with 4G services.

3.88 Session Cleanup Reporting Mechanism for Gx

Introduced in: SAPC 1.12.0

3.88.1 Description of Impacts

When the SAPC executes a Basic Session Cleanup or a Subscriber Session Cleanup for Gx, it sends a Gx RAR (with AVP `"Session-Release-Cause = UNSPECIFIED_REASON"`) to the PCEF for the Diameter session to be removed. Refer to the Availability and Scalability Facility Description for more details.

This capability is enabled by means of a configuration parameter.

3.88.2 Interface

No impact

3.88.3 Operation

Added a new attribute `enableReauthsOnCleanup` in the MOM to configure this capability, below class `AppConfig`. The Session Cleanup Reporting Mechanism is disabled by default.

3.89 Virtualization and Cloud in SAPC 1.12

Introduced in: SAPC 1.12.0

3.89.1 Description of Impacts

The following functions are supported:

— For SAPC deployments on OpenStack based NFVIs, the VM Evacuation is supported only for Traffic Processor VM type.

— Automatic Scale for OpenStack TOSCA deployments are now supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack deployments.

— Using different name for the VIM and for the ENM is now supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) in the HOT deployments in OpenStack.

3.89.2 Capacity and Performance

No impact

3.89.3 Interface

No impact

3.89.4 Operation

Regarding VM Evacuation support, the possible values for the ha-policy parameter configuration in System Controllers VMs are limited. Refer to the SAPC VNF Descriptor Generator Tool and Create VNF Package Using BCAT documents for further details.

3.90 SAPC PCF Support for IP Address Overlapping

Introduced in: SAPC 1.12.0

3.90.1 Description of Impacts

If the SAPC PCF receives two concurrent `Npcf_SMPolicyControl_Create` requests and these two PDU sessions have the same `supi` and `pduSessionId`, the SAPC PCF rejects one of the requests.

The SAPC PCF supports the following IP address overlapping scenarios:

— Support to differentiate PDU sessions for different subscribers having the same IPv4 address, the same DNN, the same SMF, but different IP domains.

— Support to differentiate PDU sessions for the same subscriber having the same IPv4 address, the same DNN, the same SMF, but different IP domains.

The SAPC PCF supports to perform Rx-N7 session binding with ipDomain supported.

For more information, refer to Dynamic Policy Control (Rx) for SAPC PCF and Access and Charging Control (N7).

3.90.2 Capacity and Performance

No impact

3.90.3 Interface

The following AVP and attributes are introduced:

- `Rx AAR`: `IP-Domain-Id` AVP is supported.
- `N7 Npcf_SMPolicyControl_Create` Request: `ipDomain` attribute is supported in Data Structure `SmPolicyContextData`.
- `N7 Npcf_SMPolicyControl_Update` Request: `ipDomain` attribute is supported in Data Structure `SmPolicyUpdateContextData`.

3.90.4 Operation

The following changes are done to Logging Events:

- Ip-Domain is added in the Rule to Install event.
- Ip-Domain is added in the Rule to Remove event.

3.91 Policy Studio 2.0

Introduced in: SAPC 1.12.0

3.91.1 Description of Impacts

New interface for Policy Studio, according to Ericsson brand 2.0, replaces old style.

Versioning starts with Policy Studio 2.0, with compatibility with SAPC 1.12

3.91.2 Capacity and Performance

No impact

3.91.3 Interface

Ericsson brand 2.0 adopted.

3.91.4 Operation

No impact

3.92 N7 Session Basic Cleanup Mechanism Updates

Introduced in: SAPC 1.12 EP1

3.92.1 Description of Impacts

The N7 session basic cleanup mechanism is updated. The SAPC introduces IP Domain (attribute IpDomain or smfId) to check the obsolete sessions in IP overlapping scenario.

Note: If the obsolete N7 session is created before upgrading to SAPC 1.12, the SAPC does not perform basic cleanup to this duplicate N7 session.

For more information, see Availability and Scalability.

3.92.2 Capacity and Performance

No impact

3.92.3 Interface

No impact

3.92.4 Operation

No impact

3.93 SAPC PCF Support of Priority and Temporary Subscription of Subscriber Groups

Introduced in: SAPC 1.12.0 EP1

3.93.1 Description of Impacts

The SAPC PCF supports temporary subscriber groups by using the subscriber group priority, and start date and end date from the UDR.

For more information, refer to Subscription and Policy Management for SAPC PCF.

3.93.2 Capacity and Performance

No impact

3.93.3 Interface

On the N36 interface, the `vendorSpecific-000193` attribute including the ExtendedSubscriberCategory data structure is added to the SmPolicyDnnData data structure.

For more information, refer to N36 Interface Description.

3.93.4 Operation

No impact

3.94 QoS Handling Mechanism Update

Introduced in: SAPC 1.12 EP3

3.94.1 Description of Impacts

The SAPC reinterprets the value `0` assigned to Maximum Bit Rate (MBR) Uplink (UL) and Downlink (DL) in QoS profile: now it means `0` (integer value), instead of 'undefined'.

This change impacts use of mbrDownlink and mbrUplink fields in QoS profiles for IP-CAN and for contents, and also MBR values calculated in previous interactions of an existing session.

Note: This reinterpretation of value `0` has important implications if this value has been used for QoS profiles in a live SAPC, as after the upgrade from a version earlier to 1.12 EP3 the flow for uploading or downloading will be cut (`0` bytes).

3.94.2 Interface

No impact.

3.94.3 Operation

No impact.

3.95 PDU Session Reauthorization Triggered by Time of Day

Introduced in: SAPC 1.12.0 EP1

3.95.1 Description of Impacts

The SAPC PCF performs PDU session reauthorization and policy evaluation triggered by Time of Day.

For more information, refer to Subscription and Policy Management for SAPC PCF.

3.95.2 Capacity and Performance

No impact

3.95.3 Interface

No impact

3.95.4 Operation

No impact

3.96 Binding Support Function

Introduced in: SAPC 1.13.0

3.96.1 Description of Impacts

The SAPC PCF provides the following functions over the Nbsf interface:

— Registering the binding information for a UE when an IPv4 address or an IPv6 prefix is allocated for a PDU session.

— Deregistering the binding information for a UE when the PDU session is released.

— BSF Geographical Redundancy (1+1).

For more information, refer to Interaction with BSF.

3.96.2 Capacity and Performance

When the traffic over the Nbsf interface is not triggered because the preconditions are not fulfilled, there is no significant impacts on the memory usage and CPU load.

When the traffic over the Nbsf interface is triggered, the following impacts need to be considered:

— The memory used by each PDU session is increased by adding the binding ID information got from the BSF.

— The extra CPU time is required to handle the operations on the Nbsf interface, which is about 22% of the CPU time for the operations on the N7 interface.

3.96.3 Interface

Nbsf is a service based interface, newly supported by the SAPC PCF.

The SAPC PCF supports messages exchanged for the following service operations over Nbsf interface:

— Nbsf_Management_Register

— Nbsf_Management_Deregister

For more information, refer to Nbsf Interface Description.

3.96.4 Operation

The following parameters are added under class PcfAppConfig in MOM:

— `PcfBsfRegAllowedLists` for registration of PDU session binding information

— `enableSessionTerminateOnBsfRegFail` to enable the PDU session termination on BSF registration failure

The following attributes are added in the `adapt_cluster.cfg` file to support traffic separation and Dual-Stack:

— HTTP2_BSF_PORT

— BSF_VIP

3.97 Access and Mobility Policy Control

Introduced in: SAPC 1.13.0

3.97.1 Description of Impacts

The Access and Mobility Policy Control (AMPC) service provides the access control and the mobility management related policies to the Access and Mobility Management Function (AMF) through the N15 interface. The AMPC adheres to the policy control framework of the 5GC architecture and its defined Npcf service based interface.

The SAPC PCF provides the following functions:

- Access and Mobility (AM) policy association establishment, modification, and termination.
- Time Of Day triggered reauthorization of the AM policy association
- Service Area Restriction (SAR)
- RAT Frequency Selection Priority (RFSP)
- Location Based Policies
- Presence Reporting Area (PRA)
- Policy Control Request Triggers Selection
- Dynamic Group Selection

For more information, refer to Access and Mobility Policy Control (N15).

3.97.2 Capacity and Performance

The capacity license of the SAPC is updated to control the AMPC sessions over N15 interface. Therefore, the active AMPC sessions created through N15 are counted in total number of active mobile sessions.

3.97.3 Interface

- N15 - The SAPC PCF supports messages exchanged for the following service operations over the N15 interface:
  - Npcf_AMPolicyControl_Create
  - Npcf_AMPolicyControl_Update
  - Npcf_AMPolicyControl_UpdateNotify for session modification

- Npcf_AMPolicyControl_Delete

The N15 interface supports traffic separation and dual-stack. The communication over the N15 interface between the SAPC and the AMF supports mTLS.

For more information, refer to N15 Interface Description.

- Nnrf - The following information is added to Nnrf interface to support configuring the SAPC PCF registration profile .
  - value `AMF` to attribute `allowedNfTypes`
  - value `npcf-am-policy-control` to attribute `serviceName`

  For more information, refer to Nnrf Interface Description.
- N36 - The following information is added to N36 Interface to support the SAPC PCF retrieves the AM data from the UDR:
  - New resource URI: `GET {apiRoot}/nudr-dr/v2/policy-data/ues/{ueId}/am-data`
  - New data type `AmPolicyData` in the `Nudr_DataRepository_Query` response and new data type `PolicyDataChangeNotification`
  - Attribute `vendorSpecific-000193` in the `AmPolicyData` data type, for retrieving priority and temporary subscription of subscriber groups from the UDR

  For more information, refer to N36 Interface Description.
- Provisioning Rest API - The following URIs are added in Provisioning Rest API:
  - `/profiles/presence-reporting-area`
  - `/profiles/presence-reporting-area/{profileId}`
  - `/profiles/service-area-restriction`
  - `/profiles/service-area-restriction/{profileId}`

  For more information, refer to Provisioning REST API.

3.97.4 Operation

The following policy tag is added:

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

The following policy types are added:

— Service Area Restriction Profile

— RFSP Selection

For more information, refer to Configuration Guide for Access and Mobility Policy Control (N15).

The following attributes are added in class PcfSecurity in MOM to support configuring mTLS:

— `enableTLSClientAuthenticationAMF`

The following parameters are added in the `adapt_cluster.cfg` file to support traffic separation and Dual-Stack:

— `HTTP2_N15_PORT`

— `N15_VIP`

For more information, refer to Adapt Cluster Tool.

The following logging events are updated to support the AMPC:

— Error Sending HTTP Request

— Error Sending HTTP Response

— Internal Error

— Protocol Error

— Timeout Receiving HTTP Response

For more information, refer to Logging Events.

The following parameters are added to support configuring SAPC PCF registration profile for the AMPC:

— `{N15_VIP}`

— `{N15_VIP_IPV6}`

— `{ampc_status}`

— `{n15_port}`

For more information, refer to Configuration Guide for Interaction with NRF.

The PDC property `amf_interface_counters` is added to `/storage/system/config/sapc/pdc.cfg` file to support configuring PDC function for the AMF.

For more information, refer to Performance Data Collection.

The following troubleshooting tools support the AMPC:

— session-handler

— pot-utility

For more information, refer to SAPC Troubleshooting Guide.

3.98 Network Repository Function Redundancy (1+1)

Introduced in: SAPC 1.13.0

3.98.1 Description of Impacts

The SAPC PCF provides an NRF 1+1 deployment:

— The SAPC PCF selects a primary NRF for traffic. When the primary NRF becomes unavailable, the SAPC PCF performs failover to the secondary NRF. When the primary NRF becomes available again, the SAPC PCF performs failback.

— In case the NRFs are unavailable or the NF discovery failed, the SAPC PCF allows to choose between using previously discovered NFs or using locally configured NFs, according to the new configuration parameter `switchToLocalNfs`.

For more information, refer to Interaction with NRF.

3.98.2 Capacity and Performance

No impact

3.98.3 Interface

No impact

3.98.4 Operation

The following changes are done to MOM:

— Allows the possibility to define two separate instances of `PcfPeerNode` with a NRF type below `PcfPeerNodes` to configure two NRFs, in the SAPC PCF.

— Added the `switchtoLocalNfs(PcfNodeType)` attribute under class `PcfAppConfig`.

The following alarm is added:

— *Policy Control, Failover Caused by Failure on NRF Connection*

3.99 Policy Studio 2.1 Improvements in SAPC 1.13

Introduced in: SAPC 1.13.0

3.99.1 Description of Impacts

User experience is improved as follows:

— Search by reference allows the user to find the referenced subject in all relevant subjects. For instance, the user can find the referenced policy in specific Dataplans

— Deletions in local changes. This allows the user to delete any SAPC object locally in the workspace. The deletion can be later committed together with any other local changes of the workspace, making the deletion effective in the SAPC when needed, and in an atomic way.

3.99.2 Capacity and Performance

No impact

3.99.3 Interface

No impact

3.99.4 Operation

No impact

3.100 Virtualization and Cloud Improvements in SAPC 1.13

Introduced in: SAPC 1.13

3.100.1 Description of Impacts

— File injection of the `adapt_cluster.cfg` configuration file to the SAPC through personality files is replaced, in a transparent way, by using the `user_data` parameter for new deployments in OpenStack. This allows the SAPC to be deployed in OpenStack environments including later releases in which personality files are no longer supported (Stein onwards).

— OVF packages are no longer supported for VNF Deployments in OpenStack.

— Ericsson Cloud Manager (ECM) is no longer supported for VNF Deployments in OpenStack. CPI procedures documented for VNF deployments are updated accordingly to describe the usage of Ericsson Orchestrator Cloud Manager (EO) instead of ECM. However, this change does not impact an earlier version SAPC (SAPC 1.12 or lower) deployed by ECM to upgrade to SAPC 1.13 or a later version by following SAPC Upgrade Instruction.

— Instantiation, manual or automatic Scaling and Termination for TOSCA deployments are supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) in OpenStack environments without NFVO (Small stack).

— Instantiation and Termination for TOSCA deployments are supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) in VMware vCloud Director environments without NFVO (Small stack).

— The use of Evolved Virtual Network Function Manager (E-VNFM) is supported for the SAPC workflows.

— Deploying SAPC PCF on VMWare NFVI by using vCloud Director is supported.

— Memory Dimensioning in PLs in a Live SAPC Operation Instructions is removed.

3.100.2 Capacity and Performance

No impact

3.100.3 Interface

No impact

3.100.4 Operation

No impact

3.101 SAPC PCF Support for Single Radio Voice Call Continuity

Introduced in: SAPC 1.13.0

3.101.1 Description of Impacts

The SAPC PCF supports the Single Radio Voice Call Continuity (SRVCC) over N7 and Rx interface which refers to transfer of an IMS Multimedia Telephony call

from the PS domain to the CS domain, when the UE can transmit and receive on only one of those access networks at a given time.

For more information, refer to Dynamic Policy Control (Rx) for SAPC PCF.

3.101.2 Capacity and Performance

No impact

3.101.3 Interface

The following changes are made to support SVRCC:

— N7

- Added the `pduSessRelCause` attribute in the `SmPolicyDeleteData` data structure of the `Npcf_SMPolicyControl_Delete` request.
- Added the `PDUSessionRelCause` supported feature.
- Added the PS_TO_CS_HAN value in the `failureCode` attribute within the `RuleReport` data type.

3.101.4 Operation

No impact

3.102 SAPC PCF Support for Voice over New Radio

Introduced in: SAPC 1.13.0

3.102.1 Description of Impacts

The SAPC PCF enables the support of Voice over New Radio (VoNR) calls.

For more information, refer to Dynamic Policy Control (Rx) for SAPC PCF.

3.102.2 Capacity and Performance

No impact

3.102.3 Interface

No impact

3.102.4 Operation

No impact

3.103 SAPC PCF Support for SM Policy Data Associated with Specific S-NSSAI and DNN Combination

Introduced in: SAPC 1.13.0

3.103.1 Description of Impacts

The SAPC PCF supports SM policy data definitions for each specific S-NSSAI and DNN combination in UDR. When the SM policy data from UDR is different for each S-NSSAI and DNN combination, the SAPC PCF is able to handle it, simultaneously applying data on the corresponding established sessions on different S-NSSAI and DNN combinations.

The SM policy data associated with specific S-NSSAI and DNN combination feature can be used only with CCDM 1.3 and EDA 2.4, and onwards.

3.103.2 Capacity and Performance

No impact

3.103.3 Interface

No impact

3.103.4 Operation

The following policy tags are added for SM policy control of the SAPC PCF:

— `AccessData.smPolicyContextData.sliceInfo.sst`

— `AccessData.smPolicyContextData.sliceInfo.sd`

3.104 Support of Subscription Removal Notifications from UDR for SM Policy Control

Introduced in: SAPC 1.13.0

3.104.1 Description of Impacts

The SAPC PCF manages notifications from UDR about removal of the following subscriber data:

— SM policy data: the SAPC PCF requests to SMF the termination of the related PDU sessions.

— Operator specific data: the SAPC PCF reauthorizes the PDU sessions and sends the updated policy decisions to the SMF.

For more information, refer to Subscription and Policy Management for SAPC PCF.

3.104.2 Capacity and Performance

No impact

3.104.3 Interface

The following attributes are added to the N36 interface:

— `supportedFeatures` (`ResourceRemovalNotificationPolicyData`) in `PolicyDataSubscription` data structure

— `delResources` in `PolicyDataChangeNotification` data structure

3.104.4 Operation

No impact

3.105 IP-CAN/PDU Session QoS Control Based on Requested QoS

Introduced in: SAPC 1.13.0 EP1

3.105.1 Description of Impacts

The SAPC can use latest received QoS parameters from PCEF or SMF in IP-CAN/PDU session QoS control, when those parameters are not defined in the calculated QoS Profile. For more information, refer to Bearer QoS and Bandwidth Management and QoS Control and Bandwidth Management (N7).

3.105.2 Capacity and Performance

No impact

3.105.3 Interface

No impact

3.105.4 Operation

To enable the function, the operator must define a QoS profile in Entity Data Source (EDS) using the received QoS values as input values. For the configuration example, refer to Configuration Guide for Bearer QoS Control and Bandwidth Management and Configuration Guide for QoS Control and Bandwidth Management (N7).

The following policy tags are added:

- `AccessData.bearer.Qos.arpPci`
- `AccessData.bearer.Qos.arpPriorityLevel`
- `AccessData.bearer.Qos.arpPvi`
- `AccessData.bearer.Qos.mbrDownlink`
- `AccessData.bearer.Qos.mbrUplink`
- `AccessData.bearer.Qos.qci`

3.106 Virtualization and Cloud Improvements in SAPC 1.14

Introduced in: SAPC 1.14

3.106.1 Description of Impacts

- The current procedure Change Geographical Redundancy to Active-Active to transform a SAPC Geographical Redundancy deployment configured as Active-Standby into Active-Active is updated to add support for VNF deployments. The procedure requires the VNF deployment to be done with VLAN-based configuration (VLAN tagging).
- Scale for TOSCA deployments is supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) in VMware vCloud Director environments with and without NFVO (Full and Small stack).
- Rollback for Upgrade Workflow is supported through the Virtual Network Function Life Cycle Manager (VNF-LCM).

— Upgrade Workflow is supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) on TOSCA deployments in OpenStack/VMware vCloud Director environments without NFVO (Full and Small stack).

— Administrative Healing is supported through the Virtual Network Function Life Cycle Manager (VNF-LCM) in preTOSCA deployments in OpenStack environments with and without NFVO (Full and Small stack).

3.106.2 Capacity and Performance

No impact

3.106.3 Interface

No impact

3.106.4 Operation

No impact

3.107 UE Trace Tool for N7

Introduced in: SAPC 1.14.0

3.107.1 Description of Impacts

The UE Trace Tool enables the operator to collect N7 incoming and outgoing messages for a set of User Equipments (UEs) in a similar way as it is done for Rx, Gx, Sd, and Sy interfaces.

3.107.2 Capacity and Performance

No impact

3.107.3 Interface

On the N7 interface the SAPC is able to:

— Activate or deactivate incoming and outgoing UE traces for a user indicated by `supi` or `gpsi` attributes

— Show UE trace sessions that are being traced

— Collect messages filtered for subscriber ID in MSISDN or IMSI format

— Schedule trace sessions

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

— Generate an xml and a pcap file containing messages from all active UE tracing sessions

3.107.4 Operation

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

For more information, refer to UE Trace Tool.

3.108 Session Cleanup Mechanism Due to Inactivity for AM Policy Association

Introduced in: SAPC 1.14.0

3.108.1 Description of Impacts

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

For more information, see Availability and Scalability.

3.108.2 Capacity and Performance

No impact

3.108.3 Interface

No impact

3.108.4 Operation

The following event logs are updated:

— Start deleting inactive sessions

— End deleting inactive sessions

3.109 Access and Mobility Policy Control Uplift to 3GPP Release 16

Introduced in: SAPC 1.14.0

3.109.1 Description of Impacts

The API version for service `Npcf_AMPolicyControl` has been updated to 1.1.0, to align with the version of OpenAPI defined in Release 16 of Technical Specification of Access and Mobility Policy Control

The presence information supports reporting the change of presence state for an area (IN_AREA, OUT_OF_AREA, INACTIVE, UNKNOWN), which produces a decrease in signaling.

The SAPC PCF supports defining Presence Area with eNodeB identifiers.

3.109.2 Capacity and Performance

No impact

3.109.3 Interface

- N15 Interface
  - Added `globalENbIdList` attribute in `PresenceInfo` data structure.
  - Added `eNbId` attribute in `GloablRanNodeId` data structure.

3.109.4 Operation

The following new policy tag over N15 Interface is added.

- `AccessData.subscriber.locationInfo.presenceReportingArea["presenceAreaName"].state`

3.110 Network Repository Function Uplift to 3GPP Release 16

Introduced in: SAPC 1.14.0

3.110.1 Description of Impacts

The API version for service Nnrf_NFManagement and Nnrf_NFDiscovery have been updated to 1.1.0 to align with the version of OpenAPI defined in Release 16 of Technical Specification of Network Repository Function.

The SAPC PCF NF services can be expressed as a map.

Array replacement is supported for attributes of type array. Both in modifications of PCF NF profile (controlled by new `enableArrayReplacement` configuration attribute), and in notifications of changes in NF profile of discovered NFs.

The SAPC PCF NF supports reporting its load information to the NRF.

3.110.2 Capacity and Performance

No impact.

3.110.3 Interface

— Nnrf_NFManagement Interface:

  • Added `nfServiceList`, `nfInstanceName`, `load`, and `loadTimeStamp` in `NFProfile` data structure.

  • Added `requesterFeatures` in `SubscriptionData` data structure.

— Nnrf_NFDiscovery Interface:

  • Added `nfServiceList` in `NFProfile` data structure.

  • Added `requester-features` in URI query parameters supported by the `GET` method.

3.110.4 Operation

In MOM, added the following configuration changes:

— Parameter `enableArrayReplacement` is added under class `PcfNrfClient`.

— The following parameters are added under class `PcfAppConfig`

  • `loadGranularity`

  • `pcfInstanceName`

3.111 Binding Support Function Uplift to 3GPP Release 16

Introduced in: SAPC 1.14.0

3.111.1 Description of Impacts

The API version for service Nbsf_Management has been updated to 1.1.0 to align with the version of OpenAPI defined in Release 16 of Technical Specification of Binding Support Function.

3.111.2 Capacity and Performance

No impact.

3.111.3 Interface

No impact.

3.111.4 Operation

No impact.

3.112 Enhancement in Session Cleanup Mechanism due to Inactivity for SM Policy Association

Introduced in: SAPC 1.14

3.112.1 Description of Impacts

Error code 404 (Not Found) is supported as an answer from SMF for a request about SM Policy Association liveness.

3.112.2 Capacity and Performance

No impact

3.112.3 Interface

No impact

3.112.4 Operation

No impact

3.113 Policy Studio 2.2 Improvements in SAPC 1.14

Introduced in: SAPC 1.14.0

3.113.1 Description of Impacts

User experience is improved as follows:

- Policy Studio provides support, not only for SAPC 1.14, but also for older versions of SAPC. Policy Studio automatically adjusts the interface to the correct data model for the SAPC version provided that the admin defined the SAPC version when defining the connection.
- Policy Studio provides support for the following products other than SAPC:
  - CCRC NSSF
- Studio Nodes

  The user can create Studio Nodes, that are workspaces not connected to any node, allowing the user to work in offline mode, on configurations that can be later imported into any real node.

For more information, refer to 5G Core Policy Studio.

3.113.2 Capacity and Performance

No impact

3.113.3 Interface

No impact

3.113.4 Operation

No impact

3.114 SAPC PCF Support for FQDN

Introduced in: SAPC 1.15.0

3.114.1 Description of Impacts

The SAPC PCF supports using the FQDNs to access:

- Nnrf services, or SBI services provided by the UDR or the BSF.

— Notification URI provided by the SMF or the AMF.

For more information, refer to HTTP/2 Connection Management.

Note: If Rolling upgrade is applied from previous SAPC PCF versions, this feature might lead to two scenarios: SM or AM Policy Association URI mismatching, which happens under the following situations:

— SM Policy Association URI mismatching

It is possible to happen if `pcfFqdn` (under `PcfAppConfig`) is configured in the SAPC PCF, and the SMF sets the SAPC PCF's IP Address as value for the `:authority` header of the `Npcf_SMPolicyControl_Create` request.

1. There are SM policy associations established, for which the SAPC PCF has answered the `Npcf_SMPolicyControl_Create` request with a `Location` header as an URI containing the IP address. This IP address is from the `:authority` header of the request.
2. A Rolling upgrade is done, and an update notify happens for some of those SM policy associations. The SAPC PCF puts an URI in the `resourceUri` field of the `Npcf_SMPolicyControl_UpdateNotify` request. Because `pcfFqdn` is configured, the URI is formed with the FQDN, not the IP address.
3. If the SMF uses the two URIs mentioned above to correlate messages from the SAPC PCF, it cannot successfully match the policy association.

   The mismatch does not happen if the SMF uses the `smPolicyId` as the key of the SM policy association.

— AM Policy Association URI mismatching

It is possible to happen if `pcfFqdn` (under `PcfAppConfig`) is configured in the SAPC PCF, and the AMF sets the SAPC PCF's IP Address as value for the `:authority` header of the `Npcf_AMPolicyControl_Create` request. Refer to *SM Policy Association URI mismatching* for details.

To avoid these mismatching scenarios, apply Single Step upgrade, so that the active policy associations are not kept.

3.114.2 Capacity and Performance

No impact

3.114.3 Interface

The SAPC PCF supports the following functions for 5G SBI interfaces including Nnrf, N7,N15,N36 and Nbsf:

— Accessing service operation URI and notification URI by FQDN, for both HTTP and HTTPs scheme.

— Verifying the `subjectAltName` attribute in the server certificate from TLS server during TLS or mTLS handshake.

3.114.4 Operation

The `requireSubjectAltNameinServerCert` attribute is added under class `PcfSecurity` in `MOM`.

For more information, refer to HTTP/2 Connection Management.

The following attributes are added under class `PcfAppConfig` in `MOM` to support traffic separation:

— `pcfFqdnNnrf`

— `pcfFqdnN7`

— `pcfFqdnN15`

— `pcfFqdnN36`

— `pcfFqdnNbsf`

For more information, refer to Configuration Guide for Interaction with NRF.

The following alarms are added:

— Policy Control, FQDN in Certificates are obsolete

— Policy Control, FQDN Convert Error

The *Additional Text* and corresponding description of alarm Policy Control, TLS Peer Server Certificate Verification Failure are updated.

The following log event is added:

— Error Getting IP Address by FQDN

3.115 Policy Studio 2.3 Improvements in SAPC 1.15

3.115.1 Description of Impacts

User experience is improved as follows:

— Policy Studio starts providing support for the following products other than SAPC:

  • CCRC NRF

— Referrers

  When viewing any object, the user can inspect which objects in the configuration are referring to it. For instance, when looking at a Rule configuration, a right panel provides information on the Policies that are using that Rule.

For more information, refer to 5G Core Policy Studio.

3.115.2 Capacity and Performance

No Impact.

3.115.3 Interface

No Impact.

3.115.4 Operation

No Impact.

3.116 SAPC PCF Support for Internal Subscription Repository

Introduced in: SAPC 1.15.0

3.116.1 Description of Impacts

The SAPC PCF supports storing the subscriber data in the internal subscription repository.

By default, the SAPC PCF works with the UDR. Use of the internal subscription repository can be selected by configuring the `pcfSubsRepository` to SPR.

The following points must be observed before configuring the subscription repository to SPR:

— The configuration must be done before the SAPC takes 5G traffic.

— The SPR mode for the SAPC PCF means only the internal subscription repository. If the SAPC works in PCF and PCRF dual mode, and the SAPC PCRF uses an external SPR for subscriber data, the external SPR is not supported as subscription repository for the SAPC PCF.

— Internal subscription repository is not supported if the SAPC PCF needs to support both SM and AM policy controls.

— In the internal subscription repository, it is not supported to provision the static policy data per S-NSSAI and DNN combination. To select different subscriber groups for different S-NSSAI and DNN combinations, dynamic group selection policies must be used.

For more information, refer to Database Access for SAPC PCF.

3.116.2 Capacity and Performance

The memory requirement and CPU usage of the SPR deployment for SM policy controls, compared with working with the UDR, is as follows:

— More static memory is required to store the subscriber data in the internal database.

— Less CPU usage and response time is required for the handling of N7 traffic because of less cost on subscriber data access.

3.116.3 Interface

No impact

3.116.4 Operation

Provisioning REST API

Support provisioning multiple `presenceReportingAreaNames` (the upper limit is 64) to a subscriber at `/subscribers/{subscriberId}/static-qualification` URI.

MOM

Added the `pcfSubsRepository` attribute under class `PcfAppConfig`.

Logging Events

The Subscriber ID in `SubsId` attribute is different for UDR and SPR modes:

— In UDR mode, the subscriber ID is the SUPI in IMSI type (with `imsi-` prefix) or the GPSI in MSISDN type (with `msisdn-` prefix).

— In SPR mode, the subscriber ID is the administrative ID (if provisioned) or the traffic ID with pure value of IMSI or MSISDN.

3.117 Aggregated UE Location Changes

3.117.1 Description of Impacts

The SAPC PCF supports the aggregated UE location changes feature and the `USER_LOCATION_CH` policy control request trigger. The `USER_LOCATION_CH` policy control request trigger indicates that user location has changed, applicable to serving area change and serving cell change.

For more information, refer to Access and Charging Control (N7).

3.117.2 Capacity and Performance

No impact

3.117.3 Interface

The following changes are done on the N7 interface:

— Added `42` (AggregatedUELocChanges) in `SupportedFeatures` data structure.

— Added `USER_LOCATION_CH` (`13`) in `PolicyControlRequestTrigger` data structure.

3.117.4 Operation

When provisioning `eventTriggers` in the `subscriber` or `dataplan` URI in the provisioning REST API:

— Only number `210` is used for the `SAREA_CH` policy control request trigger.

— Number `13` can be used for the `USER_LOCATION_CH` policy control request trigger.

3.118 Session Cleanup per Node for SMF/AMF with Session-Handler

Introduced in: SAPC 1.15.0

3.118.1 Description of Impacts

The session-handler tool is enhanced to support the N7/N15 session cleanup on a per-node basis for SMF and AMF. When removing N7 sessions for a specified SMF, the existed binding Rx/Sy sessions are removed as well.

The session-handler tool also supports to show the total number of N7/N15 sessions for the specified peer node, and the progress of an ongoing session cleanup.

For more information of session-handler, refer to SAPC Troubleshooting Guide.

3.118.2 Capacity and Performance

Running session-handler to delete sessions for a peer node needs to simulate session terminations. This simulation can increase the CPU load which can impact the ongoing traffic. Therefore, it is recommended to perform the delete action for a peer node at an off-peak time.

3.118.3 Interface

No impact

3.118.4 Operation

New option `--peerNode <peernode>` is introduced to the CLI which runs the session-handler.

The following logging events are introduced:

— Session cleanup based on node starts

— Session cleanup based on node finished

3.119 Indirect Communication (Option C) through Service Communication Proxy (SCP)

Introduced in: SAPC 1.15.0

3.119.1 Description of Impacts

For indirect communication (Option C) with target NF through the SCP, the SAPC PCF provides the following functions:

— SCP Selection based on NF Attributes

— Load Sharing among two or more serving SCPs

— Multiple hops among two or more serving SCPs

— Failover and Failback with NF (the UDR or the BSF) 1+1

— Failover to direct communication and failback to indirect communication

— Delivery of SBI service requests or notification requests through the SCP

— Supporting apiPrefix in NF configuration

For more information, refer to Indirect Communication through SCP.

The SAPC PCF also supports apiPrefix in discovered NF information. For more information, refer to Configuration Guide for Interaction with BSF and Configuration Guide for Interaction with UDR.

3.119.2 Capacity and Performance

No impact

3.119.3 Interface

The SAPC PCF supports messages routed by the SCP over N7, N15 (AMPC), N36, and Nbsf interface:

— SBI service requests and responses

— Notification requests and responses

For detailed messages supported, refer to Indirect Communication through SCP.

Added new HTTP custom headers: `3gpp-Sbi-Target-apiRoot` and `3gpp-Sbi-Callback`.

For `3gpp-Sbi-Target-apiRoot` which shall be applicable for the request sent by the SAPC PCF, the custom header is added in the following request:

— N7 interface

- `Npcf_SMPolicyControl_UpdateNotify - Modification`
- `Npcf_SMPolicyControl_UpdateNotify - Termination`

— N15 (AMPC) interface

- `Npcf_AMPolicyControl_UpdateNotify - Modification`
- `Npcf_AMPolicyControl_UpdateNotify - Termination`

— N5/N30 interface

- `Npcf_PolicyAuthorization_Notify - Notification`
- `Npcf_PolicyAuthorization_Notify - Termination`

— N36 interface

- Nudr_DataRepository_Query
- Nudr_DataRepository_Update
- Nudr_DataRepository_Subscribe
- Nudr_DataRepository_UnSubscribe

— Nbsf interface

- Nbsf_Management_Register
- Nbsf_Management_Update
- Nbsf_Management_Deregister

For 3gpp-Sbi-Callback which shall be applicable for the Notification request sent by the SAPC PCF, the custom header is added in the following request:

— N7 interface

- Npcf_SMPolicyControl_UpdateNotify - Modification
- Npcf_SMPolicyControl_UpdateNotify - Termination

— N15 (AMPC) interface

- Npcf_AMPolicyControl_UpdateNotify - Modification
- Npcf_AMPolicyControl_UpdateNotify - Termination

— N5/N30 interface

- Npcf_PolicyAuthorization_Notify - Notification
- Npcf_PolicyAuthorization_Notify - Termination

3.119.4 Operation

The following changes are done to MOM:

— Added class ScpSelectionRules to configure rules for SCP selection.

— Added attribute enableFailoverToDirectCommunication under class PcfNetwork.

— Added attribute apiPrefix under class PcfPeerNode.

— Added attribute apiPrefix under class DiscoveredPeerNode.

For more information, refer to Configuration Guide for Indirect Communication through SCP.

The following alarm is added:

— Policy Control, Connection to SCP Failed

The *Source* and *Additional Info* of the following log event is modified:

— Unsuccessful HTTP Response Received

3.120 Virtualization and Cloud Improvements in SAPC 1.15

Introduced in: SAPC 1.15.0

3.120.1 Description of Impacts

— Minimum resources for the SAPC deployment in Cloud has been modified: Minimum memory for PLs is increased from 10GB to 14GB. Upgrade procedure is provided.

3.120.2 Capacity and Performance

Minimum memory for PLs is increased from 10GB to 14GB.

Note: Minimum-size configuration is recommended for very limited number of provisioned subscribers and sessions. For accurate figures of subscribers and sessions supported, consult market support for dimensioning.

3.120.3 Interface

No impact

3.120.4 Operation

No impact

3.121 Enhancement in Session Cleanup Mechanism due to Inactivity for Rx Obsolete Sessions

Introduced in: SAPC 1.15

3.121.1 Description of Impacts

Session inactivity cleanup mechanism has been extended to remove obsolete Rx sessions.

When Session Inactivity Cleanup Mechanism starts for Gx, N7, Smp, and N15 (AMPC) sessions, all Rx sessions marked as obsolete are removed.

For more information, refer to Availability and Scalability.

3.121.2 Capacity and Performance

Cleanup time increases slightly, as Rx obsolete sessions are always considered.

3.121.3 Interface

No impact

3.121.4 Operation

No impact

3.122 QoS arpPci and arpPvi Handling Mechanism Update for N7 Interface

Introduced in: SAPC 1.15.0

3.122.1 Description of Impacts

The SAPC PCF interprets properly the values of `arpPci` and `arpPvi` in provisioned QoS profiles for N7 interface. A value of `FALSE` means 'ENABLED' (it meant 'DISABLED' previously), and a value of `TRUE` means 'DISABLED' (it meant 'ENABLED' previously).

For more information, refer to Configuration Guide for QoS Control and Bandwidth Management (N7).

After a successful upgrade from a version earlier than SAPC 1.15, the `arpPci` and `arpPvi` in QoS profiles assigned by SAPC PCF on N7 interface are evaluated based on the new logic.

For necessary actions during upgrade, refer to section *Adjust Values of arpPci and arpPvi in Provisioned QoS Profiles for N7 Interface* in SAPC Upgrade Instruction.

3.122.2 Capacity and Performance

No impact

3.122.3 Interface

No impact

3.122.4 Operation

This change affects the use of `arpPci` and `arpPvi` fields in QoS profiles at both session and content levels.

3.123 SAPC PCF Support for Subscriber Data Stored in CUDB

Introduced in: SAPC 1.16.0

3.123.1 Description of Impacts

The SAPC PCF can work with the CUDB and the CCDM simultaneously upon receiving SM policy association creation requests from the SMF. The SAPC PCF queries the CUDB or the CCDM depending on policy conditions such as the RAT type and MSISDN ranges.

Two sets of CUDBs are supported. Each CUDB set is deployed as 1+1 active-standby.

For more information, refer to Database Access for SAPC PCF.

3.123.2 Capacity and Performance

There is a little performance decrease compared with UDR mode. If `pcfSubsRepository` is configured as `DECIDE_BY_CONDITIONS` and Subscription Repository Type policies are used to select a CUDB node, additional performance loss occurs.

Runtime memory usage is less because of no cache for subscriber data.

3.123.3 Interface

No impact

3.123.4 Operation

Policy Type

Added Subscription Repository Type policy type.

MOM

Support new value `DECIDE_BY_CONDITIONS` for the `pcfSubsRepository` attribute under class `PcfAppConfig`.

Logging Events

If the subscriber data is stored in the CUDB, the subscriber ID in `SubsId` attribute is the administrative ID (if provisioned) or the traffic ID with pure value of MSISDN or IMSI.

3.124 UDR Geographical Redundancy (1+1+1)

Introduced in: SAPC 1.17.0

3.124.1 Description of Impacts

The SAPC PCF supports UDR redundancy for up to three geographically distributed UDRs (1+1+1 Primary-Secondary-Tertiary). The UDRs can be discovered from the NRF or configured in SAPC PCF locally.

If the primary UDR has an NF Set ID, the SAPC PCF selects the UDRs for failover in the same NF set. If the primary UDR has no NF Set ID, the SAPC PCF selects the UDRs for failover without NF Set ID.

3.124.2 Capacity and Performance

No impact

3.124.3 Interface

On Nnrf interface, the SAPC PCF supports UDR discovery with `target-nf-set-id` parameter, and supports the UDR status subscription with `nfSetId` condition.

3.124.4 Operation

The SAPC PCF supports to configure the UDR peer node information with `nfSetIdList` attribute in PcfPeerNode class.

3.125 BSF Geographical Redundancy (1+1+1)

Introduced in: SAPC 1.17.0

3.125.1 Description of Impacts

The SAPC PCF supports BSF redundancy for up to three geographically distributed BSFs (1+1+1 Primary-Secondary-Tertiary). The BSFs can be discovered from the NRF or configured in SAPC PCF locally.

If the primary BSF has an NF Set ID, the SAPC PCF selects the BSFs for failover in the same NF set. If the primary BSF has no NF Set ID, the SAPC PCF selects the BSFs for failover without NF Set ID.

3.125.2 Capacity and Performance

No impact

3.125.3 Interface

On Nnrf interface, the SAPC PCF supports BSF discovery with `target-nf-set-id` parameter, and supports the BSF status subscription with `nfSetId` condition.

3.125.4 Operation

The SAPC PCF supports to configure the BSF peer node information with `nfSetIdList` attribute in PcfPeerNode class.

3.126 SMF Geographical Redundancy Based on Binding Indication

Introduced in: SAPC 1.17.0

3.126.1 Description of Impacts

The support for SMF geographical redundancy aims to select an SMF for sending notifications on N7 interface. The SMF notifies the SAPC PCF of Binding Indication with the preferred SMF and NF set information. The SAPC PCF discovers all the SMFs within the NF set from the NRF.

The SAPC PCF can perform failover to an available SMF within the NF set when the preferred SMF is unavailable. The SAPC PCF can also perform failback to the preferred SMF when it is available again.

3.126.2 Capacity and Performance

To handle the Binding Indication for each session, the impacts on capacity and performance are as follows:

— The performance drop is up to 2% in TPS of the N7 traffic.

— The memory of each session is increased for saving the Binding Indication information.

3.126.3 Interface

N7

— Supports custom header `3gpp-Sbi-Binding`

— Supports HTTP causes NF_FAILOVER and NF_SERVICE_FAILOVER for `500` Internal Server Error

Nnrf

Added the following attributes or values in Nnrf_NFDiscovery_NFDiscover request:

— `SMF` in `target-nf-type`

— Service name received in Binding Indication, in `service-names`

— NF Set ID received in Binding Indication, in `target-nf-set-id`

— Bit 5 (Query-Params-Ext2) in `requester-features`

Added the following attributes and values in `subscrCond` in Nnrf_NFManagement_NFStatusSubscribe request:

— `nfSetId` attribute

Added `conditionEvent` attribute in NotificationData in Nnrf_NFManagement_NFStatusNotify request.

3.126.4 Operation

A new logging event is introduced: Binding Indication Change Received.

A new alarm is introduced for SMF connection failure: Policy Control, Connection to SMF Failed for SM Policy Control UpdateNotify.

3.127 Policy Studio Improvements in SAPC 1.17

Introduced in: SAPC 1.17

3.127.1 Description of Impacts

— Export and import with other formats. Besides the existing json format, Policy Studio can also use the resty format and the resource-list format.

For more information, refer to 5G Core Policy Studio.

3.127.2 Capacity and Performance

No Impact.

3.127.3 Interface

No Impact.

3.127.4 Operation

No Impact.

3.128 Dynamic Policy Control (N5/N30)

Introduced in: SAPC 1.17

3.128.1 Description of Impacts

The SAPC PCF provides the following functionality by the Npcf_PolicyAuthorization service to the AF and NEF:

— Feature negotiation

— Session binding

— Classification, authorization and qualification of dynamic services

— Generation of dynamic PCC rules

— Allocation of QoS information to the authorized dynamic services

— Re-evaluation of previous policy decisions taken for the PDU session

— Provisioning and removal of PCC rules and default QoS to the SMF

— Events Notification to the AF or NEF

For more information, refer to Dynamic Policy Control (N5/N30).

3.128.2 Capacity and Performance

The capacity license of the SAPC is updated to control AF sessions over N5/N30 interface. Therefore, the active AF sessions created through N5/N30 interface are counted in total number of active AF (Rx + N5/N30) sessions.

3.128.3 Interface

The SAPC PCF supports messages exchanged for the following service operations over N5/N30 interface:

— Npcf_PolicyAuthorization_Create

— Npcf_PolicyAuthorization_Update

— Npcf_PolicyAuthorization_Notify

— Npcf_PolicyAuthorization_Delete

For more information, refer to N5/N30 Interface Description.

The SAPC PCF supports messages routed by the SCP over N5/N30 interface, refer to Indirect Communication through SCP.

The SAPC PCF supports the following attributes in the Nbsf_Management_Register and Nbsf_Management_Update messages:

— `pcfFqdn`

— `pcfIpEndPoints`

For more information, refer to Nbsf Interface Description.

The following information is added to Nnrf interface to support configuring the SAPC PCF registration profile:

— value `NEF` and `AF` to attribute `allowedNfTypes` in data type `NFProfile`

— value `NEF` and `AF` to attribute `allowedNfTypes` in data type `NFService`

— value `npcf-policy-authorization` to attribute `serviceName`

For more information, refer to Nnrf Interface Description.

3.128.4 Operation

The following application (Npcf_PolicyAuthorization data) tag is newly added to the SAPC PCF:

— `AfData.media.QoSReference`

For more information, refer to Configuration Guide for Dynamic Policy Control (N5/N30).

The following changes are done to MOM:

— Added attribute `enableTLSClientAuthenticationAF` under class `PcfSecurity` (refer to HTTP/2 Connection Management for more information).

— Added attribute `pcfFqdnN5` under class `PcfAppConfig`.

— Added following tags to SAPC PCF registration profile to support Npcf_PolicyAuthorization service (refer to Configuration Guide for Interaction with NRF for more information):

  — `{N5_VIP}`

  — `{N5_VIP_IPV6}`

  — `{N5_PORT}`

  — `{PCF_FQDN_N5}`

  — `{AUPC_STATUS}`

The following attributes are added in the `adapt_cluster.cfg` file to support traffic separation and Dual-Stack:

— `HTTP2_N5_PORT`

— `N5_VIP`

For more information, refer to Adapt Cluster Tool.

The following alarms are added:

— Policy Control, Number of Npcf_PolicyAuthorization_Create Responses Sent Indicating Too Busy Reached

— Policy Control, Number of PCF response Npcf_PolicyAuthorization failure Reached

— Policy Control, Number of PCF initiated Npcf_PolicyAuthorization_Notify failure Reached

The following logs are extended with the Npcf_PolicyAuthorization protocol:

— Error Sending HTTP Request

— Error sending HTTP response

— HTTP Response Received

— HTTP Request Sent

— Protocol Error

— Timeout receiving HTTP response

— Unable to classify dynamic Service

For more information, refer to Logging Events.

The following measurements are added:

— NpcfPolAuthCreateFailed

— NpcfPolAuthCreatePDUSessionNotAvailable

— NpcfPolAuthCreateRequests

— NpcfPolAuthCreateSuccess

— NpcfPolAuthCreateTooBusy

— NpcfPolAuthDeleteFailed

— NpcfPolAuthDeleteRequests

— NpcfPolAuthDeleteSuccess

— NpcfPolAuthDeleteTooBusy

— NpcfPolAuthNotifyFailed

— NpcfPolAuthNotifyRequests

— NpcfPolAuthNotifySuccess

— NpcfPolAuthNotifyTimeout

— NpcfPolAuthRespFailed

— NpcfPolAuthServiceNotAuthorized

— NpcfPolAuthUnknownSessionId

— NpcfPolAuthUpdateFailed

— NpcfPolAuthUpdateRequests

— NpcfPolAuthUpdateSuccess

— NpcfPolAuthUpdateTooBusy

For more information, refer to Measurements.

The following KPIs are added:

- Policy Authorization Create Failure Ratio
- Policy Authorization Update Failure Ratio
- Policy Authorization Delete Failure Ratio
- Policy Authorization Notification Failure Ratio
- Policy Authorization Request Failure owing to Congestion Ratio
- Policy Authorization Request Failure owing to Service Not Authorized Ratio
- Policy Authorization Request Failure owing to Unknown Session Ratio
- Policy Authorization Transactions per Second

For more information, refer to Key Performance Indicators.

The following troubleshooting tools are supported for the Npcf_PolicyAuthorization service:

- session-handler
- pot-utility

For more information, refer to SAPC Troubleshooting Guide and SAPC Advanced Troubleshooting Guideline.

3.129 Session Cleanup per Node for Gx/Smp with Session-Handler

Introduced in: SAPC 1.17.0

3.129.1 Description of Impacts

The session-handler tool is enhanced to support the Gx/Smp session cleanup on a per-node basis for PCEF and MME. When removing Gx sessions for a specified PCEF, the existed binding Rx/Sy sessions are removed as well.

The session-handler tool also supports to show the total number of Gx/Smp sessions for the specified peer node, and the progress of an ongoing session cleanup.

For more information of session-handler, refer to SAPC Troubleshooting Guide.

3.129.2 Capacity and Performance

Running session-handler to delete sessions for a peer node needs to simulate session terminations. This simulation can increase the CPU load which can

impact the ongoing traffic. Therefore, it is recommended to perform the delete action for a peer node at an off-peak time.

3.129.3 Interface

No impact.

3.129.4 Operation

Option `--peerNode <peernode>` is used to the CLI which runs the session-handler.

3.130 Performance Data Collection Support 5G related Counters

Introduced in: SAPC 1.17.0

3.130.1 Description of Impacts

The SAPC provides Performance Data Collection (PDC) support to collect 5G traffic counter and generate output information.

The following properties have been new added for supporting 5G traffics related counters:

— smf_interface_counters

— udr_interface_counters

— bsf_interface_counters

— pol_auth_interface_counters

For more information, refer to Performance Data Collection.

3.130.2 Capacity and Performance

No impact.

3.130.3 Interface

No impact.

3.130.4 Operation

No impact.

3.131 Rebalancing of long-lived connections

Introduced in: SAPC 1.18

3.131.1 Description of Impacts

As a client, after the SAPC PCF receives the GOAWAY frame, the SAPC PCF supports to set up a new connection with the server and sends new requests on the new connection.

For the ongoing streams of the connection that receives the GOAWAY frame:

— if stream id ≤ last stream id provided in the GOAWAY frame, then the SAPC PCF waits for the ongoing streams to finish, and then terminates the connection.

— if stream id > last stream id provided in the GOAWAY frame, then the SAPC PCF closes the stream and retries the messages in a new connection or other-stayed connection. After that, the SAPC PCF closes the connection that receives the GOAWAY frame.

3.131.2 Capacity and Performance

No Impact

3.131.3 Interface

No Impact

3.131.4 Operation

No Impact

3.132 UE Trace Tool for AM Policy Control on N15 Interface

Introduced in: SAPC 1.18.0

3.132.1 Description of Impacts

The UE Trace Tool enables the operator to collect AM policy control incoming and outgoing messages on N15 interface for a set of User Equipments (UEs) in a similar way as it is done for SM policy control on N7 interface.

3.132.2 Capacity and Performance

To avoid significant performance impact, it is recommended to trace less than 10 subscribers simultaneously.

3.132.3 Interface

On the N15 interface for AM policy control, the SAPC is able to:

- Activate or deactivate incoming and outgoing UE traces for a user indicated by `supi` or `gpsi` attributes
- Show UE trace sessions that are being traced
- Collect messages filtered for subscriber ID in MSISDN or IMSI format
- Schedule trace sessions
- Display a trace in real-time using the UE Trace viewer
- Generate an xml and a pcap file containing messages from all active UE tracing sessions

3.132.4 Operation

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

For more information, refer to UE Trace Tool.

3.133 BSF Geographical Redundancy (1+1+1+1)

Introduced in: SAPC 1.18.0

3.133.1 Description of Impacts

The SAPC PCF supports BSF redundancy for up to four geographically distributed BSFs (1+1+1+1 Primary-Secondary-Tertiary-Quaternary). The BSFs can be discovered from the NRF or configured in SAPC PCF locally.

If the primary BSF has an NF Set ID, the SAPC PCF selects the BSFs for failover in the same NF set. If the primary BSF has no NF Set ID, the SAPC PCF selects the BSFs for failover without NF Set ID.

3.133.2 Capacity and Performance

No impact

3.133.3 Interface

No impact

3.133.4 Operation

To support four BSFs, the maximum number must be configured to 4.

3.134 Modifying Subscriber Operator Specific Infos by REST

Introduced in: SAPC 1.14 EP5 and SAPC 1.18

3.134.1 Description of Impacts

In Provisioning Rest API, modifying the Subscriber Operator Specific Information(OSI) is introduced:

— the whole OSI can be added, removed, or replaced by the PATCH method.

— a single entry of OSI can be added, removed, or updated by PATCH or PUT/DELETE method.

3.134.2 Capacity and Performance

No impact

3.134.3 Interface

The following changes are made to the Provisioning Rest API:

— PATCH method is introduced to Subscriber OSI interface, with the following URIs:

  • `/subscribers/{subscriberId}` (for the whole OSIs)

  • `/subscribers/{subscriberId}/operator-specific-infos` (for the element of OSIs)

— A new URI is introduced to support the adding, removing or updating of an specified OSI attribute. GET/PUT/DELETE methods are supported for this URI:

  • `/subscribers/{subscriberId}/operator-specific-infos/{attributeName}`

For more information, refer to Provisioning REST API.

3.134.4 Operation

The following measurement is introduced:

— restPatch

3.135 Policy Studio 2.6 Improvements in SAPC 1.18

Introduced in: SAPC 1.18

3.135.1 Description of Impacts

— Policy Studio, as part of the 5G Core Policy Studio strategy, is now enhanced with a higher level application, called Policy Studio Manager: this application allows the user to manage Service Cases that comprise the configuration of multiple Policy Objects in multiple Policy Decision Points at the same time. The initial Service Case is the Optimized Connectivity for Enterprise, that configures Dataplans, Policies and Rules, and AmfSets simultaneously in all the PCFs and NSSFs contained in a Slice chosen by the operator.

  For more information, refer to 5G Core Policy Studio.

3.135.2 Capacity and Performance

No impact.

3.135.3 Interface

No impact.

3.135.4 Operation

No impact.

3.136 Virtualization and Cloud Improvements in SAPC 1.18

Introduced in: SAPC 1.18 EP1

3.136.1 Description of Impacts

Resources for the SAPC deployment in Cloud has been modified:

— Minimum disk size of SC VM is increased from 40GB to 60GB.

— Memory occupied by SAPC application per TP VM is reduced.

3.136.2 Capacity and Performance

Minimun disk size of SC VM is increased from 40 GB to 60 GB.

Additional 5 GB memory per TP VM is available.

3.136.3 Interface

No impact.

3.136.4 Operation

No impact.

3.137 Support of Subscription Removal Notifications from UDR for AM Policy Control

Introduced in: SAPC 1.19

3.137.1 Description of Impacts

The SAPC PCF manages notifications from UDR about removal of AM policy data:

— the SAPC PCF sends update notification requests to the AMF for the termination of AM policy association session.

For more information, see Subscription and Policy Management for SAPC PCF.

3.137.2 Capacity and Performance

Slight memory impact due to storing time-stamp of the AM session creation and session status.

Slight performance impact caused by additional tasks to handle the termination of the AM policy association.

3.137.3 Interface

— N15 Interface

The SAPC PCF supports messages exchanged for the following service operations:

- Npcf_AMPolicyControl_UpdateNotify for session termination

For more information, see N15 Interface Description.

— N36 Interface

Added `delResources` support for the removal of AM policy data.

3.137.4 Operation

`enableReauthsOnSubsChange` is extended to apply to N15 session.

3.138 5G Core Policy Studio Improvements in SAPC 1.19

Introduced in: SAPC 1.19

3.138.1 Description of Impacts

— Policy Studio changes its denomination to 5G Core Policy Studio. The version that follows Policy Studio 2.6 is 5G Core Policy Studio 3.0.

— 5G Core Policy Studio contains 2 applications: Policy Configurator comprising the traditional features from Policy Studio, and Policy Manager comprising new features for template-based, multi-node configuration. This beta delivery of Policy Manager allows the definition of Slices as groups of Policy NFs, where the user can deploy configurations based on parameterized Templates, called Services. The Service is a deployment of such configuration onto all the NFs in the Slice.

— Import errors reporting. In case of a large number of errors when importing a big file, the user can extract a report in a cvs format. This export can be used to examine all the errors and warnings detected by Policy Studio before applying the import effectively.

3.138.2 Capacity and Performance

No impact.

3.138.3 Interface

No impact.

3.138.4 Operation

No impact.

3.139 UE Policy Control

Introduced in: SAPC 1.19.0

3.139.1 Description of Impacts

With the UE Policy Control service (SAPC PCF as service producer) and AMF Communication service (SAPC PCF as service consumer), the SAPC PCF provides UE policy to the UE through AMF. The SAPC PCF supports only UE Route Selection Policy (URSP) as the UE policy.

The SAPC PCF provides the following functions:

— UE policy association establishment, modification and termination

— UE policy selection, encoding, and delivery

For more information, see UE Policy Control (N15).

3.139.2 Capacity and Performance

The capacity license of the SAPC is updated to control the UE sessions over N15 interface. Therefore, the active UE sessions created through N15 are counted in total number of active mobile sessions.

3.139.3 Interface

N15 Interface

The SAPC PCF supports the following service operations:

— Npcf_UEPolicyControl service:

    - Npcf_UEPolicyControl_Create
    - Npcf_UEPolicyControl_Update
    - Npcf_UEPolicyControl_Delete

— Namf_Communication service:

    - N1N2MessageSubscribe
    - N1N2MessageTransfer
    - N1MessageNotify
    - N1N2TransferFailureNotification
    - N1N2MessageUnsubscribe service operations

The services support traffic separation and dual stack. The communication over N15 interface between the SAPC and the AMF supports mTLS.

Added HTTP header `3gpp-Sbi-Lci` in the following response:

— Npcf_UEPolicyControl_Create

— Npcf_UEPolicyControl_Update

— Npcf_AMPolicyControl_Delete

For more information, see N15 Interface Description.

N36 Interface

The following information is added to support retrieval of UE policy set from the UDR:

— New resource URI: `GET {apiRoot}/nudr-dr/v2/policy-data/ues/{ueId}/ue-policy-set`

— New data type UePolicySet in Nudr_DataRepository_Query response

For more information, see N36 Interface Description.

Nnrf Interface

The following is added:

— `npcf-ue-policy-control` service in NFRegister operation.

— `nfInstanceId` attribute in `subscrCond` attribute of NFStatusSubscribe operation.

— `target-nf-instance-id` attribute, `AMF` value in `target-nf-type` attribute, and `namf-comm` value in `service-names` attribute of NFDiscover operation.

For more information, see Nnrf Interface Description.

Provisioning REST API

The following URIs are added:

— `/profiles/ursp`

— `/profiles/ursp/{profileId}`

For more information, see Provisioning REST API.

3.139.4 Operation

In MOM, a new class `UePolicyControl` is added, which includes the following attributes:

— `uePolicyT3501Timer`

— `n1N2UePolicyReattemptDelay`

— `n1N2MessageMaxReattempts`

For detailed configuration of UE Policy Control, see Configuration Guide for UE Policy Control (N15).

The following alarms are added:

— Policy Control, Connection to AMF Failed for Namf_Communication Service

— Policy Control, Connection to UDR Failed for UE Policy Control

— Policy Control, Number of Npcf_UEPolicyControl Responses Sent Indicating Failure Reached

— Policy Control, Number of Npcf_UEPolicyControl_Create Responses Sent Indicating Too Busy Reached

— Policy Control, Number of Npcf_UEPolicyControl_Update Responses Sent Indicating Too Busy Reached

— Policy Control, Number of Npcf_UEPolicyControl_Delete Responses Sent Indicating Too Busy Reached

NpcfUe Protocol Measures and NamfComm Protocol Measures are added. For details, see Measurements.

The following key performance indicators are added:

— UE Policy Control Create Failure Ratio

— UE Policy Control Update Failure Ratio

— UE Policy Control Delete Failure Ratio

— UE Policy Control Transactions per Second

— UE Policy Control N1 Messages Transfer per Second

— UE Policy Control N1 Messages Transfer Failure Notification per Second

— UE Policy Control N1 Messages Notification per Second

For details, see Key Performance Indicators.

The following troubleshooting tools are supported for UE Policy Control:

— session-handler

— pot-utility

For more information, see SAPC Troubleshooting Guide and SAPC Advanced Troubleshooting Guideline.

3.140 UE Policy Control through SCP

Introduced in: SAPC 1.19.0

3.140.1 Description of Impacts

For UE Policy Control through SCP, the SAPC PCF provides the following functions:

— Delivery of SBI service requests through the SCP over N15(UEPC) interface for the Npcf_UEPolicyControl service.

3.140.2 Capacity and Performance

No impact

3.140.3 Interface

For N15 (UEPC) interface, added HTTP header `3gpp-Sbi-Target-apiRoot` in the following request:

— `N1N2MessageSubscribe`

— N1N2MessageTransfer

— N1N2MessageUnsubscribe

3.140.4 Operation

No impact

3.141 Inactive Session Cleanup for UE Policy Association

Introduced in: SAPC 1.19.0

3.141.1 Description of Impacts

The SAPC PCF provides an automatic cleanup mechanism to remove all the obsolete UE Policy Association sessions.

A session is considered inactive or obsolete when no Npcf_UEPolicyControl request is received or no notification sent in inactive period time.

For more information, see Availability and Scalability.

3.141.2 Capacity and Performance

No impact

3.141.3 Interface

The SAPC PCF supports the following message exchange service operations over N15 interface for inactive UE policy association session cleanup if check alive is configured:

— Npcf_UEPolicyControl_UpdateNotify

For more information, see N15 Interface Description.

3.141.4 Operation

The following measurements are added:

— NpcfUeUpdateNotifyFailed

— NpcfUeUpdateNotifyRequests

— NpcfUeUpdateNotifySuccess

For more information, see Measurements.

The following event logs are updated to add N15 UEPC sessions:

— Start deleting inactive sessions

— End deleting inactive sessions

For more information, see Logging Events.

The following new attributes are added in the class `UePolicyControl` in MOM:

— `checkForUePolicySessionAlive`

— `uePolicyInactivityPeriod`

3.142 Temporarily Inactive PCC Rules

Introduced in: SAPC 1.19.0

3.142.1 Description of Impacts

The SAPC PCF supports the Charging-Rule-Report AVP with parameter `PCC-Rule-Status=TEMPORARILY INACTIVE` in Gx interface

For more information, see Access and Charging Control (Gx)

3.142.2 Capacity and Performance

No impact

3.142.3 Interface

Support for temporarily inactive PCC rule status in Gx Interface.

3.142.4 Operation

The following new policy tag over Gx and Rx Interface is added:

— `AccessData.subscriber.service["serviceName"].isOutOfCredit`

3.143 OCS selection based on Charging Characteristic received over N7

Introduced in: SAPC 1.19.0

3.143.1 Description of Impacts

The SAPC PCF supports to provide received charging Characteristics by policy tag `AccessData.Subscriber.chargingChars` over N7 interface. The same policy tag is already supported over Gx interface.

3.143.2 Capacity and Performance

No impact

3.143.3 Interface

No impact

3.143.4 Operation

The following policy tag is added over N7 interface:

— `AccessData.subscriber.chargingChars`

3.144 Support of New QCI/5QI Values

Introduced in: SAPC 1.19.0

3.144.1 Description of Impacts

The SAPC supports the following new 3GPP Release16 QCI/5QI values:

— 71,72,73,74,76 for Enhanced Framework for Live Uplink Streaming

— 86 for Enhanced V2X Service

For details, see Bearer QoS and Bandwidth Management and QoS Control and Bandwidth Management (N7).

3.144.2 Capacity and Performance

No impact

3.144.3 Interface

No impact

3.144.4 Operation

No impact

3.145 Usage Monitoring Control (N7) Enhancements in SAPC 1.19

Introduced in: SAPC 1.19.0

3.145.1 Description of Impacts

Note: The Usage Monitoring Control (N7) enhancements are applicable when the subscription repository is SPR. For more information on database access, see Database Access for SAPC PCF.

The SAPC PCF supports enhancements to the usage monitoring control function of Session Management Policy Control through the N7 interface.

The SAPC PCF provides the following functions:

— Fair Usage Profiles defined on shared subscriber plans

— Force usage reporting from SMF

— Monitoring key selection

— Get usage limits and write usage accumulation in CUDB/CCDM

— Time usage monitoring control

— Types of usage limits: complementary limits, session limits, conditional limits, intermediate limits

— Prepaid subscription type

— Minimum quota volume, slice volume and reporting interval time

— Accumulate usage depending on conditions

— Shared devices plans support

3.145.2 Capacity and Performance

No impact

3.145.3 Interface

Provisioning REST API

The following URIs are reused to provision usage monitoring profiles and usage accumulators:

— `/dataplans/{dataplanId}/usage-limits`

— `/subscribers/{subscriberId}/usage-accumulators`

— `/subscribers/{subscriberId}/usage-limits`

— `/shared-dataplans`

— `/shared-dataplans/{sharedDataplanId}`

— `/shared-dataplans/{sharedDataplanId}/usage-accumulators`

The following URI is reused to provision Monitoring Key for preconfigured and dynamic services unconditionally:

— `/contents/{contentName}/static-qualification`

For more information, see Provisioning REST API.

N7 Interface

The `lastReqUsageData` attribute with RequestedUsageData data type is added in SmPolicyDecision in Npcf_SMPolicyControl_UpdateNotify Requests.

3.145.4 Operation

The SAPC PCF supports the following policy types:

— Conditional Accumulation

— Conditional Accumulation for Multiple Counters

— Monitoring Key

The SAPC PCF supports the following policy tags:

— Fair Usage Related Tags

- `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].current["type"]`
- `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].currentPercentage["type"]`

- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].expiryDate["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].hasExpired["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].isActive["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].isLimitSurpassed["type"][n]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].remaining["type"][n]
- AccessData.subscriber.receivedUsage.reportingGroup ["total"/"reportingGroupName"].usageType["type"]
- AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].current["type"]
- AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"]/ "reportingGroupName"].currentPercentage["type"]
- AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].isLimitSurpassed["type"][n]
- AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].remaining["type"][n]

Fair Usage Related Tags, Multiple Usage Accumulators:

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].current["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].currentPercentage["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].expiryDate["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].isLimitSurpassed["type"][n]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].remaining["type"][n]

- AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].counter["counterName"].current["type"]
- AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].counter["counterName"].currentPercentage["type"]
- AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].counter["counterName"].isLimitSurpassed["type"][n]
- AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].counter["counterName"].remaining["type"][n]

Fair Usage Related Tags, Multiple Service Offerings:

- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].current["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].currentPercentage["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].expiryDate["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].remaining["type"][n]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].current["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].currentPercentage["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].expiryDate["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].hasExpired["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].remaining["type"][n]

- `AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].current["type"]`
- `AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].currentPercentage["type"]`
- `AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].remaining["type"][n]`
- `AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].current["type"]`
- `AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].currentPercentage["type"]`
- `AccessData.subscriber.session.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].remaining["type"][n]`

For more information, see Configuration Guide for Usage Monitoring Control with SPR (N7).

The following changes are done for Event-Based Monitoring:

- The values of MONITORING_KEY and QUOAT_TIME_DURATION are set in the USAGE_MONITORING_REPORTING_QUOTA_GRANTED event.
- The values of MONITORING_KEY and FAIR_USAGE_TIME_DURATION are set in the USAGE_ REPORTING_ACCUMULATED_USAGE event.
- The values of ACTIVESUBSCRIBEGROUP, MONITRING_KEY, COUNTER, LIMIT_TYPE, LIMIT_VALUE, and SUBSCRIPTION _TYPE are set in the USAGE_MONITORING_ LIMIT_SURPASSED event.
- The values of ACTIVESUBSCRIBEGROUP, MONITRING_KEY, SUBSCRIPTION _TYPE, and COUNTER are set in the USAGE_MONITORING_ACCUMULATED_USAGE_RESET event.

For more information, see Event-Based Monitoring.

3.146 Legacy Mode of Diameter Communication on Sy/ESy Interface

Introduced in: SAPC 1.19.0

3.146.1 Description of Impacts

Besides already supported normal mode on Sy/ESy interface, the SAPC also supports legacy mode of Diameter communication. The choice of normal mode or legacy mode is configurable in the SAPC.

Legacy mode is applicable to active-active geographical redundancy deployment. If failover occurs, with legacy mode, the SAPC always includes the Origin-Host that was used in the session establishment instead of its own Origin-Host when sending Sy/ESy messages. See Active-Active Geographical Redundancy for details.

3.146.2 Capacity and Performance

No impact

3.146.3 Interface

There is no change to the Sy/ESy-interface AVPs. The value of Origin-Host AVP is affected by the legacy mode.

3.146.4 Operation

The configuration is on the `cdiameter.origin_host_profile.sy` attribute of the `/cluster/storage/system/config/sapc/subs-charging-proc.cfg` file.

3.147 Security Management Improvements in SAPC 1.19

Introduced in: SAPC 1.19.0

3.147.1 Description of Impacts

The password for root user is changed. For more information, please see Security Hardening Guide.

3.147.2 Capacity and Performance

No impact

3.147.3 Interface

No impact

3.147.4 Operation

No impact

3.148 SAPC PCF recoveryTime Support in pcfBinding Improvement

Introduced in: SAPC 1.19

3.148.1 Description of Impacts

Starting from SAPC 1.13, the `recoveryTime` in `pcfBinding` data structure was supported, however the time zone was calculated wrongly because of no adaption according to the daylight saving time (DST) if exist.

In SAPC 1.19, the `recoveryTime` calculation is fixed with the DST consideration. But it may cause the backward compatible problem in case the start time or last restart time of SAPC just happened during the DST of local time zone, the different `recoveryTime` will be sent to the BSF after the upgrade. To solve this problem, the only way is to make a SAPC restart really to clean up all the existing sessions and apply a new `recoveryTime` of SAPC.

3.148.2 Capacity and Performance

No impact

3.148.3 Interface

No impact

3.148.4 Operation

No impact

3.149 5G Core Policy Studio 3.2 Improvements in SAPC 1.20

Introduced in: SAPC 1.20

3.149.1 Description of Impacts

The underlying database software is migrated to an SQL system based on PostgreSQL

For more information, see 5G Core Policy Studio.

3.149.2 Capacity and Performance

No Impact.

3.149.3 Interface

No Impact.

3.149.4 Operation

No Impact.

3.150 5G Core Policy Studio 3.3 Improvements in SAPC 1.20

Introduced in: SAPC 1.20

3.150.1 Description of Impacts

Rules output advanced edition: this feature allows to define rule output values with full expressions. It is available for rules whose rule output comprises:

- PCC Rules
- Profile/Content Filtering ID
- Profile/Content Monitoring Key
- SPID
- Maximum Allowed TAs

Entity sources error prevention: Policy Studio provides a syntactic and semantic validator to facilitate the creation of entity sources.

Entity sources references: Policy Studio allows to identify which rules are using an Entity source, and when creating a rule, it provides guidance to use properly each Entity source.

3.150.2 Capacity and Performance

No impact.

3.150.3 Interface

No impact.

3.150.4 Operation

No impact.

3.151 5G Core Policy Studio 3.4 Improvements in SAPC 1.20

Introduced in: SAPC 1.20

3.151.1 Description of Impacts

Entities Sources support is improved with new features:

— Validation and help for references in an Entity Source directing to another Entity Source.

— Validation and help for Entity Sources usage inside Rules conditions.

3.151.2 Capacity and Performance

No Impact.

3.151.3 Interfaces

No impact.

3.151.4 Cloud Environment

No requirements.

3.151.5 Hardware

No requirements.

3.151.6 Other Network Elements

No requirements.

3.152 QCI Change Not Restricted by QoS-Upgrade AVP for GPRS

Introduced in: SAPC 1.20.0

3.152.1 Description of Impacts

For GPRS access, QCI change is not treated as "QOS Upgrade" and not controlled by QoS-Upgrade AVP.

For details, see Bearer QoS and Bandwidth Management.

3.152.2 Capacity and Performance

No impact

3.152.3 Interface

No impact

3.152.4 Operation

No impact

3.153 Allow Any PTI Value Received in UE STATE INDICATION

Introduced in: SAPC 1.20 CP1

3.153.1 Description of Impacts

When the UE STATE INDICATION is received in UE policy association establishment request:

— The SAPC PCF accepts any PTI value in the UE STATE INDICATION.

— The SAPC PCF avoids using the above PTI value in MANAGE UE POLICY COMMAND.

3.153.2 Capacity and Performance

No impact.

3.153.3 Interface

No impact.

3.153.4 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
- rxAaasInitEmergencyFailed
- rxAaasInitEmergencySuccess
- rxAaasUnauthorizedNonEmergency

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:

- ldapSearchRequests
- ldapModifyRequests
- ldapSearchResponsesFailed
- ldapModifyResponsesFailed
- soapExtDbNotificationsReceived

— soapExtDbNotificationResponsesFailed

4.4 Mobility Based Policy Control for Overlay Deployments

Introduced in: SAPC 1.0, SAPC 1.4

4.4.1 Mobility Based Policy Control for Overlay Deployments in SAPC 1.0

4.4.1.1 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.

4.4.1.2 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.

4.4.1.3 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.

4.4.1.4 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

4.4.2 Mobility Based Policy Control for Overlay Deployments Enhancements in SAPC 1.4

4.4.2.1 Description of Impacts

Due to the enhancements, the following functions are supported:

— IP-CAN session access control

— SPID selection at Smp session modification and reauthorization

— Smp-presence Reporting Area

— Event Triggers Selection

— Integration with Online Charging System for Monetary Spending Limit Reporting

— Massive Session Cleanup and Session Cleanup Mechanism Due to Inactivity

4.4.2.2 Capacity and Performance

— Additional SAPC processing, memory and network messages are introduced for the new functions.

— New capacity license is introduced to control the number of active Smp sessions.

  When the SAPC receives CCR-U or CCR-T messages for the sessions that are established before the SAPC is upgraded to SAPC 1.4, the SAPC rejects the messages with DIAMETER_UNKNOWN_SESSION_ID result code to trigger new session establishment.

4.4.2.3 Interface

— Supports Smp RAR and RAA messages

— Supports `Event-Trigger` and `Presence-Reporting-Area-Information` AVPs in Smp CCR and CCA messages

— Supports `3GPP-MS-TimeZone` AVP in CCR messages

— Added DIAMETER_UNKNOWN_SESSION_ID (5002) and DIAMETER_AUTHORIZATION_REJECTED (5003) result codes in Smp CCA messages

4.4.2.4 Operation

Before upgrading to SAPC 1.4, make sure that the license key file is updated by including the Smp capacity license. Otherwise, the Smp traffic fails with error codes.

The following policy types are supported over Smp:

— IP-CAN Session Access Control

— Presence Reporting Area Selection

— Event Triggers Selection

The following policy tag is added:

— `AccessData.subscriber.locationInfo.presenceReportingArea["presenceAreaName"].isInArea`

The existing Smp measures are renamed: prefix sx changed to smp. The sx-measures can still be used but will be deprecated in the future.

The following Smp measures are added:

— smpCcasRejected

— smpCcasTerminateTooBusy

— smpCcasUnableToComply

— smpCcasUpdateTooBusy

— smpRaas

— smpRaasFailed

— smpRaasSuccess

— smpRaasUnableToDeliver

— smpRaasUnknownSessionId

— smpRars

— smpRarsTimeout

The following capacity measure is added:

— smpActiveGlobalSessions

The following log events are modified for the Smp interface:

— Diameter incoming message discarded

— Diameter peer node restarted

— End deleting inactive sessions

— End deleting old sessions

— Error sending CCA

— Error sending RAR

— Internal error

— Protocol error

— Start deleting inactive sessions

— Start deleting old sessions

— Timeout receiving RAA

— Unsuccessful RAA received

The Policy Control, Number of Sx CCAs Initial Sent Indicating Too Busy Reached alarm is renamed to:

— Policy Control, Number of Smp CCAs Initial Sent Indicating Too Busy Reached

The following alarm is added:

— Policy Control, Number of Smp Session Rejections Reached

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

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 Aggregable Dataplans for Fair Usage Policies

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.

4.14 Support of Sd for Application Detection and Control

Introduced in: SAPC 1.2

4.14.1 Description of Impacts

The support of Sd for Application Detection and Control (ADC) introduces the Sd interface between the SAPC and the Traffic Detection Function (TDF) that enables PCC decisions based on the reporting of detected applications from the TDF.

4.14.2 Interface

The Sd interface is a new interface between the TDF and the SAPC to provide application detection and control. For more detailed information, refer to Sd Interface Description.

Additionally to the introduction of the Sd interface, the following changes are also made in the Gx interface to support Sd:

— Added `TDF-Information` AVP (AVP code 1087) in the Gx CCR-Initial message

4.14.3 Operation

The following policy tags are added:

— Sd ADC qualification tag:

  • `TdfData.tdfApp["id"].isStarted`

— Sd dynamic classification tags:

  • `TdfData.tdfAppId`

  • `TdfData.tdfAppInstanceId`

  • `TdfData.serverIp`

  • `TdfData.serverPort`

The following policy type is added:

— Dynamic Service Classification for Sd

The following Rule Combination Algorithm is added for Sd Dynamic Service Classification:

— any-match

The following Sd measurements are added:

— sdAdcStartEvents

— sdAdcStopEvents

— sdCcasInvalidInfo

— sdCcasSuccess

— sdCcasTerminateSuccess

- sdCcasUnableToComply
- sdCcasUnknownSession
- sdCcasUpdateSuccess
- sdCcasUpdateTooBusy
- sdCcrsTerminate
- sdCcrsUpdate
- sdRaasFailed
- sdRaasSuccess
- sdRaasUnknownSessionId
- sdRars
- sdRarsTimeout
- sdTsasFailed
- sdTsasSuccess
- sdTsrs
- sdTsrsTimeout

The following capacity counter is added:

- sdActiveSessions

The following log events are added or modified for the Sd interface:

- Diameter incoming message discarded
- Error sending CCA
- Error sending RAR
- Error sending TSR
- Internal error
- Protocol error
- Timeout receiving RAA
- Timeout receiving TSA

— Unsuccessful RAA received

— Unsuccessful TSA received

4.15 Multimedia Priority Services

Introduced in: SAPC 1.2

4.15.1 Description of Impacts

The MPS function allows service users (certain government and emergency management officials and other authorized users) to obtain higher priority access to system resources over other users in congestion situation. This function includes support for subscription-based MPS and on-demand MPS. For details, see Emergency and Multimedia Priority Services.

In overload situation, the SAPC prioritizes MPS events over events handled with lower priority which are rejected or discarded. For more information, see Overload Control.

4.15.2 Interface

— Rx: supports the `MPS-Identifier` AVP

— Provisioning REST API: added the following:

- `/profiles/multimedia-priority-services` URI
- `/profiles/multimedia-priority-services/{profileId}` URI
- `mpsProfileId` attribute in the `/subscribers/{subscriberId}/static-qualification` URI

4.15.3 Operation

For subscription-based MPS, it is needed to provision MPS profiles for the subscriber. To prioritize Gx MPS events, APNs corresponding to MPS types defined in the MPS profiles must be configured.

It is possible to set the relative priority of emergency and multimedia priority services for overload control.

Added the following policy tags:

— `AccessData.subscriber.service["serviceName"].media.type["mediaType"].isRunning`

— `AccessData.subscriber.service["serviceName"].media.type["mediaType"].reservationPriority`

— `AccessData.subscriber.service["serviceName"].reservationPriority`

— `AfData.mpsIdentifier`

— `Apns.epsBearerIds`

— `Apns.imsIds`

— `Subscriber.mpsProfile.mpsType`

— `Subscriber.mpsProfile.priorityLevel`

Added the following logging event:

— IMS Multimedia Priority Service

Added the following measurements:

— `gxCcasInitMultimediaPriorityTooBusy`

— `gxCcasUpdateMultimediaPriorityTooBusy`

— `rxAaasInitMultimediaPriorityFailed`

— `rxAaasInitMultimediaPriorityTooBusy`

— `rxAaasMultimediaPrioritySuccess`

— `rxAaasUpdateMultimediaPriorityTooBusy`

— `rxAarsMultimediaPriority`

4.16 Extended Bit Rates over Gx/Rx

Introduced in: SAPC 1.2

4.16.1 Description of Impacts

Extended bandwidth AVPs representing bit rates in kbps are introduced to manage bandwidth values higher than 2^{32}-1 bps (4,3 Gbps), to support EPC Dual Connectivity (E-UTRAN and 5G NR).

4.16.2 Interface

— Gx:

  • The following new AVPs are added to the `QoS-Information` AVP in Gx CCR/RAR messages:

  - Extended-APN-AMBR-DL (AVP code 2848).
  - Extended-APN-AMBR-UL (AVP code 2849).
  - Extended-Max-Requested-BW-DL (AVP code 554).
  - Extended-Max-Requested-BW-UL (AVP code 555).
  - Extended-GBR-DL (AVP code 2850).
  - Extended-GBR-UL (AVP code 2851)
- New Supported-Features AVP instance with Feature-List-ID = 2, to support Extended-BW-NR (bit 7).

— Rx:

- The following new AVPs are added to the Media-Component-Description and Media-Sub-Component AVPs in AAR messages:
  - Extended-Max-Requested-BW-UL (AVP code 554).
  - Extended-Max-Requested-BW-DL (AVP code 555).
- New Supported-Features AVP instance with Feature-List-ID = 2, to support Extended-Max-Requested-BW-NR (bit 1).

4.16.3 Operation

The following tags are enhanced to support MBR extended values:

— AccessData.requestedQos.mbrUplink

— AccessData.requestedQos.mbrDownlink

4.17 Quota Rollover

Introduced in: SAPC 1.3

4.17.1 Description of Impacts

The Quota Rollover function enables users to spend the data not used at the end of the current period during the next one. The SAPC computes rollover data dynamically at the beginning of next billing cycle. Thus, during the next billing cycle the data usage limit for a given user would be the data usage limit entitled in the subscription plus the rollover data from previous period. Note that unused data are only rollover to next period, but not to subsequent ones.

4.17.2 Interface

The following optional attributes are added to the usage limits of reporting groups of the subscribers and dataplans REST API resources:

— `useRolloverFirst`

— `rolloverLimit`

The following optional attributes are added to the subscriber usage accumulator REST API resource:

— `useRolloverFirst`

— `rollover`

The following attribute is modified inside the subscriber usage accumulator REST API resource:

— `version` increased from value "2.2" to "2.3"

4.17.3 Operation

The following Policy tags have changed, owing to rollover quota support:

— `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].current["type"]`

— `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].currentPercentage["type"]`

— `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].remaining["type"]`

— `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].isLimitSurpassed["type"]`

— `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].current["type"]`

— `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].currentPercentage["type"]`

— `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].remaining["type"]`

— `AccessData.subscriber.accumulatedUsage.reportingGroup["total"/ "reportingGroupName"].counter["counterName"].isLimitSurpassed["type"]`

- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].current["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].currentPercentage["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].remaining["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].current["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].currentPercentage["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].remaining["type"]

New Policy tags for Quota Rollover are added:

- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].currentRollover["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].isRolloverSurpassed["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].rolloverFromPreviousPeriod["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].currentRolloverPercentage["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].counter["counterName"].currentRollover["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].counter["counterName"].isRolloverSurpassed["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].counter["counterName"].rolloverFromPreviousPeriod["type"]
- AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].counter["counterName"].currentRolloverPercentage["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].currentRollover["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].isRolloverSurpassed["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].rolloverFromPreviousPeriod["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].currentRolloverPercentage["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].currentRollover["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].isRolloverSurpassed["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].rolloverFromPreviousPeriod["type"]

— AccessData.subscriber.accumulatedUsage.reportingGroup["total"/"reportingGroupName"].group["groupName"].counter["counterName"].currentRolloverPercentage["type"]

The following log events are added:

— Rollover limit surpassed

The following log events are modified:

— Reset of accumulated usage data.

  The following attributes are added:

  • RolloverBiDir

  • RolloverUL

  • RolloverDL

  • RolloverTime

— Usage Limit Surpassed: log is also triggered when rollover quota has been consumed (`rolloverAccumulated` reaches `rolloverFromPreviousPeriod`) and `useRolloverFirst` = false.

4.18 EBM Analytics

Introduced in: SAPC 1.3

4.18.1 Description of Impacts

The EBM function provides support in the SAPC for a near realtime interface which allows the streaming of events from the SAPC to one or several EBM servers. The SAPC sends EBM event reports based on the information received from the Gx and Rx interfaces.

4.18.2 Capacity and Performance

According to measurements, the impacts of EBM on performance are the following:

— When events for the Gx interface to be reporting through EBM are configured, the performance drop of the Gx traffic regarding the baseline is 9%.

— When events for the Rx interface to be reporting through EBM are configured, the performance drop of the Rx traffic regarding the baseline is 9%.

4.18.3 Interface

The EBM interface is a new interface between the SAPC and the EBM server. For more detailed information, refer to Event-Based Monitoring Interface Description.

4.18.4 Operation

The following measurements are added:

— ebmBusinessEvents

— ebmBusinessEventsNotSent

The following alarms are added:

— Policy Control, EBM Buffer Overflow

— Policy Control, EBM Communication Failure

The following log event is added:

— EBM mandatory parameter missed

4.19 Support of New QCI for Low Latency Services

Introduced in: SAPC 1.3

4.19.1 Description of Impacts

The SAPC provides support to the new 3GPP Rel-15 QoS Class Identifiers (QCI) defined for the low latency services required by 5G (E-UTRAN and E-UTRAN-NR Dual Connectivity).

4.19.2 Capacity and Performance

No impact

4.19.3 Interface

No impact

4.19.4 Operation

The `resourceType` optional parameter in the `content-qos` profile allows the configuration of QCI values according to the 3GPP Rel-15 technical specifications.

The following QCI values are added:

— Non-GBR QCI

  80 for Low latency eMBB TCP/UDP based applications and Augmented Reality

— GBR QCI

  67 for Mission Critical Video user plane

  82 and 83 for Discrete Automation

  84 for Intelligent Transport Systems

  85 for High Voltage and Remote Control

4.20 Stackable Dataplans

Introduced in: SAPC 1.3

4.20.1 Description of Impacts

The SAPC enables the operator to activate automatically multiple vouchers with the same absolute volume or time limits for prepaid subscriptions. This is enabled by defining multiple sets of start date and end date in the association of subscriber and subscriber group. Therefore, the subscriber can use multiple times the same usage limits from the prepaid subscriptions associated with multiple instances.

4.20.2 Interface

The following optional attribute is added to the subscriber dataplan REST API resource:

— `durations`

The following optional attributes are added to the subscriber usage accumulator REST API resource:

— `instanceInUse`

— `overlapInstanceUsed`

4.20.3 Operation

The following policy tags are added:

— `AccessData.subscriber.accumulatedUsage.group["groupName"].currentInstance`

— `AccessData.subscriber.accumulatedUsage.group["groupName"].isInstanceAvailable`

— `AccessData.subscriber.accumulatedUsage.group["groupName"].newInstanceStart`

4.21 External Database Redundancy Pool Loadsharing

Introduced in: SAPC 1.4

4.21.1 Description of Impacts

The SAPC allows to define multiple access points towards the CUDB system in each of the CUDB sites. One site consists of several CUDB nodes, each one identified with one CUDB FE VIP address.

4.21.2 Capacity and Performance

As the SAPC shares the LDAP traffic between several CUDB nodes in one site instead of only one per CUDB site, the dimensioning of the UDC system may be affected due to a more even distribution of the load.

4.21.3 Interface

No impact.

4.21.4 Operation

The following alarm is added:

— Policy Control, Failover Caused by Failure on External Repository Connection

4.22 VoLTE Roaming S8HR

Introduced in: SAPC 1.5

4.22.1 Description of Impacts

VoLTE Roaming S8HR enables the SAPC to report PLMN changes from the access network to the AF. If the AF subscribes to the PLMN identifier change successfully, the SAPC provides the change information to the AF when the SAPC receives it from the PCEF.

Note: The SAPC also provides the PLMN Id within the `3GPP-SGSN-MCC-MNC` AVP in the `AA-Answer` message whenever the SAPC has requested to be updated about PLMN identifier changes and has the information available, even if the AF has not subscribed to PLMN change notification.

In case that the AF has no IMS-level roaming interfaces, the AF might request the SAPC to provide the EPC-level identities (MSISDN, IMSI, or IMEI(SV)) as part of the establishment of an IMS emergency registration or an IMS emergency session establishment.

For details, refer to sections *IMS Emergency Sessions for Roaming Users* and *IMS Emergency Sessions for Roaming Users* in the Emergency and Multimedia

Priority Services document and the *PLMN Information Change Notification* section in the Dynamic Policy Control (Rx) document.

4.22.2 Capacity and Performance

— PLMN change notification is supported at IMS SIP registration or IMS SIP call negotiation.

  Impact in the traffic model:

  — It increases the frequency of Gx and Rx operations to report PLMN changes to the AF node.

  — If the PLMN change notification is required at IMS SIP registration, the additional Rx diameter session other than the one for IMS SIP call will be established. 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.

— EPC-Level identities request is supported at IMS emergency registration or an IMS emergency session establishment.

  Impact in the traffic model:

  — If the EPC-Level identities information is requested at IMS emergency registration, the additional Rx diameter session other than the one for IMS emergency session will be established. 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.

4.22.3 Interface

— Gx

  • Added the `3GPP-SGSN-MCC-MNC` AVP to the RAA message.

— Rx

  • Added the `AF-Requested-Data` AVP in the AAR message.

  • Added the `User-Equipment-Info` and `Subscription-Id` AVPs in the AAA message.

  • Added bit value 19 (`PLMNInfo`) in the `Feature-List-ID` 1 of the `Supported-Features` AVP in AAR and AAA messages.

  • Added the `PLMN_CHANGE` (16) value to the `Specific-Action` AVP in AAR and RAR messages.

  • Added the `3GPP-SGSN-MCC-MNC` AVP in the AAA message.

4.22.4 Operation

No impact

4.23 EBM for Sy

Introduced in: SAPC 1.5

4.23.1 Description of Impacts

The EBM for Sy function provides EBM events related to the 3GPP Sy interface and the Ericsson Sy interface.

4.23.2 Capacity and Performance

According to measurements, the impact of EBM for Sy on performance is the following:

— When events for the Sy interface to be reporting through EBM are configured, the performance drop of the Sy traffic regarding the baseline is 6%.

4.23.3 Interface

With the introduction of EBM for Sy, the following events can be sent through the EBM interface:

— SY_SLR_SLA_TRANSACTION

— SY_SNR_SNA_TRANSACTION

— SY_STR_STA_TRANSACTION

4.23.4 Operation

No impact

4.24 Refillable Dataplans

Introduced in: SAPC 1.5.1

4.24.1 Description of Impacts

The SAPC enables the operator to activate automatically multiple instances with the same volume or time limits in a billing cycle for postpaid subscriptions. This

is enabled by defining instances contracted for the subscriber groups associated with the subscribers. The subscribers can receive notifications on the use of the instances and are charged by the number of instances that they have started at the end of the billing cycle. Adding, changing or removing `startDate` refills the dataplan by resetting the number of `instancesContracted`.

4.24.2 Capacity and Performance

No impact

4.24.3 Interface

The following optional attribute is added to the subscriber dataplans, dataplans, and shared dataplans in Provisioning REST API resources:

— `instancesContracted`

The following optional attribute is added to the subscriber usage-accumulators and shared dataplan usage-accumulators in Provisioning REST API resources:

— `instanceStarted`

The following attribute is modified inside the subscriber usage-accumulators and shared dataplan usage-accumulators in Provisioning REST API resources:

— version increased from value "2.3" to "2.4"

4.24.4 Operation

The following policy tags are added:

— `AccessData.subscriber.accumulatedUsage.group["groupName"].instanceStarted`

— `AccessData.subscriber.accumulatedUsage.group["groupName"].instanceRemained`

4.25 RAA with Non-Success Result-Code AVP

Introduced in: SAPC 1.5.1

4.25.1 Description of Impacts

The SAPC can be configured to remove the Gx session and any other Rx, Sy, or Sd bound session in case a Gx RAA message is received with a non-success Result-Code AVP.

Note: This behavior does not apply to:

- `DIAMETER_UNABLE_TO_DELIVER` (3002),
- `DIAMETER_TOO_BUSY` (3004),
- `DIAMETER_OUT_OF_SPACE` (4002) in case diameter race condition feature is enabled.

4.25.2 Capacity and Performance

No impact

4.25.3 Interface

Gx:

- Added `DIAMETER_LIMITED_SUCCESS` (2002) value in `Result-Code` AVP in RAA messages.

4.25.4 Operation

No impact

4.26 Forwarding of Audit Logs

Introduced in: SAPC 1.5.1

4.26.1 Description of Impacts

This function enables the forwarding of System Controller audit logs to an external server.

If configured, the rsyslog feature forwards the audit log records to a remote server, over TCP.

4.26.2 Capacity and Performance

No impact

4.26.3 Interface

No impact

4.26.4 Operation

No impact

4.27 Performance Data Splitter

Introduced in: SAPC 1.6

4.27.1 Description of Impacts

This function enables Performance Management files (PMF) in additional sub-directories. This allows the activation of PM jobs with Multi-Granularity Periods, even when some consumers of such PMF only support single Granularity Period (GP) files.

Performance Data Splitter (PDS) is disabled by default.

4.27.2 Interface

No impact

4.27.3 Operation

No impact

4.28 LDAP Central Authentication and Authorization

Introduced in: SAPC 1.6

4.28.1 Description of Impacts

This function provides user authentication and authorization through an external LDAP server for the following OAM interfaces:

— NETCONF/COM CLI

— REST API

— SFTP

— SSH

4.28.2 Capacity and Performance

No impact

4.28.3 Interface

No impact

4.28.4 Operation

The `LdapAuthenticationMethod` class is added to the MOM for the configuration of this function.

4.29 Access Network Charging Identifier

Introduced in: SAPC 1.4

4.29.1 Description of Impacts

Access Network Charging Identifier (AN-CID) function enables the SAPC to report the access network charging identifier to the AF during session establishment or session modification for adding one or more media components.

The Access Network Charging Identifier Report is a mechanism that provides the access network charging identifier of the user to the IMS network. Its main function is to correlate CDRs from elements in packet core with IMS CDRs.

4.29.2 Capacity and Performance

The AN-CID is requested during an AF session establishment. When the PCEF assigns the AN-CID for the dynamic PCC rules, the PCEF reports the Access Network Charging Identifier as a new `CCR-Update` message.

The activation of this functionality increases the number of messages exchanged between SAPC and other nodes in the network (Incoming Gx:CCR-U message reporting the Access Network Charging Information that triggers an outgoing Rx:RAR message towards the AF). The CPU load that the SAPC has to withstand increases because of the increasing number of the exchanged messages.

4.29.3 Interface

— Gx:

  • Added the `CHARGING_CORRELATION_EXCHANGE` (28) value in the `Event-Trigger` AVP in `RAR`, `CCA`, and `CCR-Update` messages.

- Added the `Charging-Correlation-Indicator` AVP (AVP code 1073) in the `Charging-Rule-Install` AVP in `RAR` messages.
- Added the `Access-Network-Charging-Identifier-Gx` AVP (AVP code 1022) in `CCR-Update` messages.

— Rx:

- Added the `CHARGING_CORRELATION_EXCHANGE` (1) value to the `Specific-Action` AVP in `AAR` and `RAR` messages.
- Added the `Access-Network-Charging-Identifier` AVP (AVP code 502) in `RAR` message.

4.29.4 Operation

No impact.

4.30 RAN NAS Cause

Introduced in: SAPC 1.7.0

4.30.1 Description of Impacts

RAN NAS Cause enables the SAPC receiving the detailed Radio Access Network (RAN) and Network Access Server (NAS) release causes from the PCEF. The PCEF receives RAN and NAS release cause code information from the access network in 3GPP-EPS access type.

4.30.2 Capacity and Performance

No impact

4.30.3 Interface

— Gx

- Added the `RAN-NAS-Release-Cause` AVP in Gx CCR messages.
- Added support for bit 22 (`RAN-NAS-Cause`) in the `Supported-Features` AVP.

— RX:

- Added the `RAN-NAS-Release-Cause` AVP in Rx RAR and Rx STA messages.

- Added support for bit 9 (`RAN-NAS-Cause`) in the `Supported-Features` AVP.

4.30.4 Operation

No impact

4.31 N+1 Geographical Redundancy

Introduced in: SAPC 1.7.5

Disclaimer: N+1 Geographical Redundancy is a fully restricted feature. All N+1 related content has been included in official documentation in order to maintain a single documentation track. This feature cannot be enabled without proper approval.

4.31.1 Description of Impacts

Geographical Redundancy deployment in an N+1 redundancy mode is implemented to have N+1 standalone SAPC peers. The IP-CAN session data including all Rx bound sessions is stored in one SAPC node, and a replica copy is stored in another SAPC peer. All N+1 SAPC peers are able to handle traffic simultaneously, although they do not store a copy of that data. No specific SAPC peer is configured to keep the replica copy. This replica peer is selected at the IP-CAN session establishment, assuring a homogeneous distribution.

Only VoLTE scenario is supported for N+1 Geographical Redundancy deployments.

4.31.2 Capacity and Performance

In a N+1 Geographical Redundancy deployment, the memory impact for storing the replica of the session is the same as in an Active-Active GeoRed deployment, maximum for the particular case of a 1+1 deployment. Because of the homogeneous distribution of the replica copy, the memory impact is less if the number of the SAPC peers is greater than one.

The N+1 Geographical Redundancy incoming Diameter traffic load balancing model is delegated on the external Diameter client distribution algorithm between the SAPC peers. For the optimal performance, the external Diameter client should select the same SAPC peer for a specific UE registration, and the associated Diameter session establishments and updates (session and subscriber stickiness), since the SAPC peers are stateful for Diameter sessions.

4.31.3 Interface

No impact

4.31.4 Operation

The following log events are added for N+1 Geographical Redundancy:

— Collision Detection Control Failure Updating Session Data

— Error Fetching Session Data from SAPC Peer

— Error Writing Session Data into SAPC Peer

The following alarm is added for N+1 Geographical Redundancy:

— Policy Control, Geographical Redundancy Provisioning Failure

The following alarm is updated for N+1 Geographical Redundancy:

— Policy Control, Geographical Redundancy Unable To Reach Peer

4.32 Special Handling Mechanism of RESOURCE_ALLOCATION_FAILURE

Introduced in: SAPC 1.8.0

4.32.1 Description of Impacts

When this function is activated by setting the `enableRxRARNotifOnAllSDFsInactive` parameter to `true`, the SAPC supports sending an `RAR` message to the AF over the Rx interface when all the Service Data Flows (SDFs) within the AF session are inactive. The AF gets notifications of the indication of release of bearer, or the indication of failed resources allocation, or both.

When the `enableRxRARNotifOnAllSDFsInactive` parameter is set to `false`, and all the SDFs within the AF session are inactive, the SAPC sends an `ASR` message to the AF.

4.32.2 Capacity and Performance

No impact

4.32.3 Interface

— Rx:

  • The Specific Handling Mechanism of `RESOURCE_ALLOCATION_FAILURE` allows the SAPC to send an `RAR` message instead of an `ASR` message to the AF over the Rx interface, when the `enableRxRARNotifOnAllSDFsInactive` parameter is set to `true`.

4.32.4 Operation

No impact

4.33 EBM: Parameters Added to RX_AAR_AAA_TRANSACTION Event

Introduced in: SAPC 1.8.0

4.33.1 Description of Impacts

The following parameters are added to the `RX_AAR_AAA_TRANSACTION`:

`MEDIA_COMPONENT_EXTENDED_QOS`

— `MEDIA_COMPONENT_NUMBER`

— `[EXTENDED_MAX_REQUESTED_BW_UL]`

— `[EXTENDED_MAX_REQUESTED_BW_DL]`

4.33.2 Capacity and Performance

No impact

4.33.3 Interface

No impact

4.33.4 Operation

No impact

4.34 QoS Handling Mechanism Enhancement

Introduced in: SAPC 1.8.0

4.34.1 Description of Impacts

The SAPC supports storing the initial QoS information in the CCR message by setting the `enableQosEnhancements` parameter to true: If the QoS profile is not permitted during the QoS evaluation, then the stored QoS information is used in the `CCA` and `RAR` messages.

4.34.2 Capacity and Performance

No impact

4.34.3 Interface

No impact

4.34.4 Operation

The following parameter is added in the `AppConfig` class in MOM:

— `enableQosEnhancements`

4.35 IP-Domain-Id enhancement

Introduced in SAPC 1.8.0

4.35.1 Description of Impacts

The SAPC implements a direct mapping to binding an Rx session with a Gx session using the `Origin-Host-Id` of the PCEF. This feature is used with any kind of PCEF configuration including cluster configuration and the Default PCEF.

Refer to the Configuration Guide for Access and Charging Control (Gx) and the Configuration Guide for Dynamic Policy Control (Rx) for details.

4.35.2 Capacity and Performance

No impact

4.35.3 Interface

— Rx

  • When the AF sends an AAR including the `IP-Domain-Id` AVP to bind AF sessions with Gx sessions, the `ipDomainId` attribute of the `DiameterNode` configuration of the PCEF is used. With the Rx session binding extension the `Origin-Host-Id` of the PCEF is used as `IP-Domain-Id` in a direct mapping when the configuration has no value for the `ipDomainId` attribute.

4.35.4 Operation

To use the direct mapping, the PCEF configuration must not define the `ipDomainId` attribute. In the Default PCEF configuration the `ipDomainId` attribute is definable but ignored.

4.36 Disable Notification of Bearer Events to the AF

Introduced in SAPC 1.9.0

4.36.1 Description of Impacts

To reduce signaling processing loads, the SAPC supports disabling notification of bearer events to the AF.

The SAPC supports disabling the following notifications:

— Service Data Flow Deactivation

— Successful Resources Allocation

— Network Location Information

— IP-CAN Type Change

— Signaling Path Status

— Access Network Charging Identifier (AN-CID)

— PLMN Information Change

The AF subscribes to notification of bearer events by using the `Specific-Action` AVP including corresponding values. By adding the specific action values in the `disabledSpecificActions` list, the corresponding notifications can be disabled.

4.36.2 Capacity and Performance

No impact

4.36.3 Interface

— Gx RAR: notification-related AVPs and values are not included when the corresponding notifications are disabled.

— Rx RAR: not sent when the corresponding notifications are disabled.

Refer to Dynamic Policy Control (Rx) for details.

4.36.4 Operation

Added new disabledSpecificActions attribute in the PccConfig class in the MOM. The list of allowed values is as follows:

— CHARGING_CORRELATION_EXCHANGE

— INDICATION_OF_RELEASE_OF_BEARER

— IP_CAN_CHANGE

— INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION

— INDICATION_OF_FAILED_RESOURCES_ALLOCATION

— ACCESS_NETWORK_INFO_REPORT

— PLMN_CHANGE

4.37 Provisioning REST API Updates

Introduced in: SAPC 1.9.0

4.37.1 Description of Impacts

For the provisioning REST API, the SAPC supports filtering contents by adding the `Description` attribute in the `<CONTENTS_URI>`.

4.37.2 Capacity and Performance

No impact

4.37.3 Interface

No impact

4.37.4 Operation

No impact

4.38 Analytics REST API Updates

Introduced in: SAPC 1.9.0

4.38.1 Description of Impacts

For the analytics REST API, the SAPC also supports using the `/subscribers/{subscriberId}/subscriber-info` URI to get the following information of the subscribers:

— PeerId

— TrafficSessionId

— MSISDN

— IMEI

4.38.2 Capacity and Performance

No impact

4.38.3 Interface

No impact

4.38.4 Operation

No impact

4.39 Configuration of the Replication Method in Geographical Redundancy Active-Active

Introduced in: SAPC 1.9

4.39.1 Description of Impacts

In Active-Active Geographical Redundancy, it is possible to configure the used replication method. The choice is a trade-off, during session establishment, between consistency and performance. For more information, refer to *Locally and Non-Locally Created Objects* in Active-Active Geographical Redundancy.

4.39.2 Interface

No impact

4.39.3 Operation

The operator can select between replication methods at installation time by modifying the stickiness parameters in `adapt_cluster.cfg` file. For more information, refer to Adapt Cluster Tool. During an upgrade procedure, the selected behavior prevails.

The behavior can be switched on demand between both geographical redundant modes. For more information, refer to Change Geographical Redundancy Replication Method.

4.40 Overload Protection in Geographical Redundancy Active-Active

Introduced in: SAPC 1.9 EP1

4.40.1 Description of Impacts

Temporary differences between databases in both Active-Active SAPCs can affect traffic handling in the preferred node. An optional overload protection feature can be enabled to minimize possible impacts. Refer to Active-Active Geographical Redundancy for more information.

4.40.2 Interface

No impact

4.40.3 Operation

The overload protection mechanism generates these new logs:

— The data mirroring is overloaded. The SAPC will handle the traffic while it replicates data from the peer.

— The data mirroring is overloaded. The SAPC will handle traffic and the SAPC peer is ACTIVE.

4.40.4 Other Impacts

The mated peer will stop handling traffic during the overload procedure.

4.41 Diameter Proxy

Introduced in: SAPC 1.9 EP1

4.41.1 Description of Impacts

The SAPC enhances the diameter stack to support diameter fail-over between SAPC peers. When broken connectivity is detected in one SAPC peer, the diameter request is relayed to the mated peer through the diameter proxy and sent out through the diameter stack of the mated peer.

This feature works only in Active-Active Geographical Redundancy deployments. For more information, see Active-Active Geographical Redundancy (Facility Description).

4.41.2 Capacity and Performance

In lab environment (2SC+10PL), when the Gx traffic VIP is disabled (worst case, all Gx connectivity is broken), a slight performance drop (less than 5%) is possible in normal VoLTE call cases.

4.41.3 Interface

The following SAPC-initiated messages are supported by diameter proxy:

— Gx RAR

— Rx RAR, ASR

— Sy SLR, STR

— Sd TSR, RAR

— Smp(Sx) RAR

4.41.4 Operation

This feature is enabled by default.

4.42 N+1 Geographical Redundancy in SAPC 1.9.5

Introduced in: SAPC 1.9.5

Disclaimer: N+1 Geographical Redundancy is a fully restricted feature. All N+1 related content has been included in official documentation in order to maintain a single documentation track. This feature cannot be enabled without proper approval.

4.42.1 Description of Impacts

N+1 Geographical Redundancy in SAPC 1.9.5 includes geographical redundancy support for Sd sessions and Fair Usage data. The usage limit data is totally replicated as part of the subscriber profile in all the SAPC nodes in the N+1 cluster, and the usage accumulator is stored only in two SAPC nodes (the primary and the replica copy), similarly to the legacy session data mirroring.

4.42.2 Capacity and Performance

In an N+1 Geographical Redundancy deployment, the memory impact for storing the Sd session replica copy is the same as in an Active-Active Geographical Redundancy deployment, maximum for the particular case of a 1+1 deployment.

If the Fair Usage Control feature is used, the memory impact for storing the replica of the usage accumulator is slightly higher than in an Active-Active Geographical Redundancy deployment, because apart from the usage accumulator replica copy, an additional index is used for each subscriber to indicate which SAPC node stores the primary copy and which SAPC node stores the replica copy in the N+1 cluster. This additional index is totally replicated, similarly to the provisioning data.

4.42.3 Interface

No impact

4.42.4 Operation

The following alarm is updated for N+1 Geographical Redundancy in SAPC 1.9.5:

— Policy Control, Geographical Redundancy Unable to Reach Peer

The following log events are modified for N+1 Geographical Redundancy in SAPC 1.9.5:

— `Error Fetching Session Data from SAPC Peer` is updated to `Error Fetching Data from SAPC Peer`

— `Error Writing Session Data from SAPC Peer` is updated to `Error Writing Data from SAPC Peer`

4.43 Overload Protection of Priority Services for SAPC PCF

Introduced in: SAPC 1.10.0 with Limited Availability, SAPC 1.11.0 with General Availability

4.43.1 Description of Impacts

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

When overloaded, the SAPC PCF does the following:

— Rejects incoming messages to reduce its load answering with 503 Service Unavailable

— Does not send request messages to the NRF

For more information, see Overload Control.

4.43.2 Interface

No impact

4.43.3 Operation

The following alarms are added:

— Policy Control, Number of Npcf_SMPolicyControl_Create Responses Sent Indicating Too Busy Reached

— Policy Control, Number of Nnrf_NFManagement_NFStatusNotify Responses Sent Indicating Too Busy Reached

4.44 IP-CAN Type Change Notification Support by SAPC PCF

Introduced in: SAPC 1.11.0

4.44.1 Description of Impacts

IP-CAN Type Change Notification enables the SAPC PCF to report access 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 PCF provides the change information to the AF when the SAPC PCF gets it from the SMF.

4.44.2 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 N7 operations.

4.44.3 Interface

— N7

- Added the `accessType`, `servNfId` (`anGwAddr`) attributes in SmPolicyContextData of Npcf_SMPolicyControl_Create Request, SmPolicyUpdateContextData of Npcf_SMPolicyControl_Update Request, and UeCampingRep of Npcf_SMPolicyControl_UpdateNotify Response.
- Added `AC_TY_CH` and `SCNN_CH` in SmPolicyDecision (`policyCtrlReqTriggers`) of Npcf_SMPolicyControl_Create Response, of Npcf_SMPolicyControl_Update Response, of Npcf_SMPolicyControl_UpdateNotify Request, and SmPolicyUpdateContextData (`repPolicyCtrlReqTriggers`) of Npcf_SMPolicyControl_Update Request.

— Rx

- Added `IP-CAN-Type` AVP with value `3GPP-5GS (8)` in RAR and AAA messages.
- Added mapping table for IP-CAN types and access types.

4.44.4 Operation

Added support of `AC_TY_CH (7)` and `SCNN_CH (211)` policy control request triggers.

Added support of `AccessData.bearer.ipCanType` policy tag for access type `8: 3GPP-5GS`.

4.45 SAPC PCF Integration with OCS

Introduced in: SAPC 1.11.0

4.45.1 Description of Impacts

The SAPC PCF performs policy and charging control based on the information received from the Online Charging System (OCS).

During N7 session establishment and modification, the SAPC PCF determines whether information from the OCS is needed to calculate the data to install in the SMF. If it is so, the SAPC PCF first selects the OCS, then sends a request to the selected one and uses the received information, together with the subscriber data retrieved from the UDR, to decide the data to install in the SMF.

The SAPC PCF can be integrated with OCS through the Sy interface and with Ericsson OCS through the Esy interface.

4.45.2 Capacity and Performance

No impact

4.45.3 Interface

The SAPC PCF handles the Sy or Esy messages by binding the Sy or Esy session with the N7 session from the SMF.

`Subscription-Id` AVP to interact with the OCS is obtained by extracting IMSI or MSISDN from SUPI or GPSI values provided by the SMF in N7 requests.

4.45.4 Operation

The operation for 5G subscribers is the same with 4G, except that the SAPC PCF does not support static provisioning of OCS at subscriber level.

4.46 Diameter Proxy Uses the Replication Channel

Introduced in: SAPC 1.11

4.46.1 Description of Impacts

The Diameter Proxy feature was introduced in SAPC 1.9 EP1 where SAPC peers communicated through the application channel (via the Traffic VIP). From SAPC 1.11, the replication channel is used instead (via the Replication VIP). This may impact on datacenter firewall configuration. For more information, see SAPC Network Description Guide.

For more information about this feature, see Active-Active Geographical Redundancy (Facility Description).

4.46.2 Capacity and Performance

No impact

4.46.3 Interface

No impact

4.46.4 Operation

No impact

4.47 5G Auto Provisioning

Introduced in: SAPC 1.11

4.47.1 Description of Impacts

The 5G Auto Provisioning function supports automatically migrating 4G subscriber data from the CUDB to the UDR by sending an EDA CAI3G SOAP notification to EDA 2. This function is used when the SAPC PCF establishes an SM Policy Association for a 4G subscriber who attaches to the 5GC Network for the first time.

For more information, refer to 5G Auto Provisioning.

4.47.2 Capacity and Performance

When the SAPC PCF establishes an SM Policy Association for a 4G subscriber who stores in the CUDB and attaches to the 5GC network for the first time, the `Npcf_SMPolicyControl_Create` response time is increased because of:

— The SAPC PCF sends an extra message SOAP CAI3G Notification to the EDA 2.

— The SAPC PCF sends an Nudr_DataRepository_Query request to the UDR to retrieve the Session Management Policy Data several times in a period.

4.47.3 Interface

No impact

4.47.4 Operation

A new attribute `enable5GAutoProvisionNotification` is introduced to MO Class `PcfAppConfig`.

4.48 SAPC PCF Support for User Notifications by SMS

Introduced in: SAPC 1.12.0

4.48.1 Description of Impacts

The SAPC PCF supports notifying an end user or external system of certain events by SMS, same as that is possible for the SAPC PCRF. The precondition is that the traffic request sent from the SMF to the SAPC PCF contains a valid MSISDN identifier in GPSI.

For more information, refer to User Notifications.

4.48.2 Capacity and Performance

The request and response time for 5G traffic is not affected by the user notifications because the notification policies are evaluated after a request or response is sent.

The TPS of 5G traffic is affected because the policy evaluation and the handling of SMPP messages consumes some CPU time and network resources.

4.48.3 Interface

The SAPC PCF uses SMPP protocol to connect with the SMS server, same as SAPC PCRF.

4.48.4 Operation

The same notification policies for the SAPC PCRF also apply to the SAPC PCF.

Provisioning `smsDestinations` to a subscriber is not applicable to the SAPC PCF.

For more information, refer to Configuration Guide for End User Notifications.

4.49 5G Auto Provisioning Updates

Introduced in: SAPC 1.12

4.49.1 Description of Impacts

The SAPC introduces the following process changes to reduce the traffic load toward the UDR:

— The SAPC establishes the SM Policy Association with Unknown Subscriber profile.

— The SAPC performs 5G Auto Provisioning immediately after the SM Policy Association establishment.

— The SAPC only queries the UDR once after the Auto Provisioning Notification is sent to the EDA 2.

For more information, refer to 5G Auto Provisioning.

4.49.2 Capacity and Performance

When a 4G subscriber attaches to the 5GC Network for the first time, the `Npcf_SMPolicyControl_Create` response time is decreased because of the number of times to query the UDR is reduced to one.

Impact in the traffic model: additional `Npcf_SMPolicyControl_UpdateNotify` message to the SMF after performing 5G Auto Provisioning.

4.49.3 Interface

No impact

4.49.4 Operation

A new attribute `PcfAutoProvisionUDRQueryTimer` is introduced to MO Class `PcfAppConfig`.

The following counters have been introduced:

— PcfAutoProvisioningNotificationsSent

— PcfAutoProvisioningNotificationsFailed

The following event logs have been introduced:

— Pcf Auto Provisioning Notification Discarded

— Pcf Auto Provisioning Notification Sent

— Unable to Deliver 5G Auto Provisioning Notification

The following parameters have been removed from the CFG file configuration:

— max_retry_UDR_query

— retry_UDR_query_interval

For more information, refer to Configuration Guide for 5G Auto Provisioning.

4.50 SAPC PCF Support for Geographical Redundancy Active-Standby

Introduced in: SAPC 1.13.0

4.50.1 Description of Impacts

The SAPC PCF supports Geographical Redundancy deployments in Active-Standby mode, where the active SAPC PCF processes the incoming traffic and provisioning operations. The standby SAPC keeps the state of the active SAPC to be ready to process the incoming traffic and provisioning operations when the active one cannot handle it. For more information, refer to Active-Standby Geographical Redundancy.

4.50.2 Interface

No impact

4.50.3 Operation

Both SAPC PCF peers must be configured with the same registration profile to allow them both to behave as the same NF instance in the network.

4.51 Analytics REST API Enhancement

Introduced in: SAPC 1.13.0

4.51.1 Description of Impacts

The Get Session Information by IMSI and Get Session Information by IP Address resources are added, enabling the operator to query session information of all the ongoing sessions by:

— IMSI, APN (if available) and PCEF (if available)

— IP address, APN (if available) and PCEF (if available)

The retrieved session information includes the following attributes:

— imsi: IMSI

- ipaddr: IP address
- apn: APN identifier
- pcef: PCEF identifier
- gxCreationTime: creation time
- gxModificationTime: modification time
- gxDiamSessionId: diameter session identifier

4.51.2 Capacity and Performance

No impact

4.51.3 Interface

The following new URIs are added to the Analytics Rest API:

For Get Session Information by IMSI

- `/sessions/subscriber/{imsi}/sessions-list`
- `/sessions/subscriber/{imsi}/sessions-list?apn=[APN]&pcef=[PCEF]`

For Get Session Information by IP Address

- `/sessions/ipaddr/{ipaddr}/sessions-list`
- `/sessions/ipaddr/{ipaddr}/sessions-list?apn=[APN]&pcef=[PCEF]`

The Translate session IP address to IMSI resource in Analytics REST API is renamed Get IMSI by IP Address.

4.51.4 Operation

No impact

4.52 SAPC PCF Support for Emergency Services

Introduced in: SAPC 1.13.0

4.52.1 Description of Impacts

The SAPC PCF supports emergency PDU sessions and IMS emergency calls of Emergency Services functionality. And the Overload control is supported for emergency services over N7 interface.

Note: IMS emergency call for roaming user is not supported.

For more information, refer to Emergency and Multimedia Priority Services and Overload Control.

4.52.2 Capacity and Performance

No impact

4.52.3 Interface

The following changes are made to support emergency services:

— N7: Added the `invalidSupi` attribute in the `SmPolicyContextData` data structure of the `Npcf_SMPolicyControl_Create` request.

4.52.4 Operation

The following measurements are added:

— NpcfSmCreateEmergencyFailed

— NpcfSmCreateEmergencySuccess

— NpcfSmCreateEmergencyTooBusy

— NpcfSmUpdateEmergencyTooBusy

— pduAuthenticatedEmergencyActiveSessions

— pduUnauthenticattedEmergencyActiveSessions

— pduEmergencyActiveSessionsPerDnn

4.53 MultiSIM Support for Sy/ESy

Introduced in: SAPC 1.13

4.53.1 Description of Impacts

The SAPC enhances the SLR of the Sy/ESy interface to help OCS identifying the same Subscriber from multiple IMSI.

When the MSISDN and IMSI come from Gx interface, or the GPSI and SUPI from N7 interface, and `SubsIdType` configuration parameter below `PccConfig` class in the MOM is configured to "`IMSI`" then the `Subscription-Id` AVP of SLR in Sy/ESy interface will include both IMSI and MSISDN.

For more information, refer to Integration with OCS for Monetary Spending Limit Reporting (Sy).

4.53.2 Capacity and Performance

No impact.

4.53.3 Interface

Both IMSI and MSISDN could be included in Subscription-Id AVP of SLR in the Sy/ESy interface.

4.53.4 Operation

No impact.

4.54 SAPC PCF Support for Disable Notification of Bearer Events to the AF

Introduced in: SAPC 1.13

4.54.1 Description of Impacts

The SAPC PCF supports disabling the following notification of bearer events to the AF.

— Service Data Flow Deactivation

— Successful Resources Allocation

— IP-CAN Type Change

For more information, refer to Dynamic Policy Control (Rx) for SAPC PCF.

4.54.2 Capacity and Performance

No impact

4.54.3 Interface

No impact

4.54.4 Operation

The notification to be disabled for the SAPC PCF is configured in `disabledSpecificActions` attribute in the PccConfig class in the MOM which is same as the SAPC PCRF. The SAPC PCF supports the following allowed values:

— INDICATION_OF_RELEASE_OF_BEARER

— IP_CAN_CHANGE

— INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION

— INDICATION_OF_FAILED_RESOURCES_ALLOCATION

For more information, refer to Configuration Guide for SAPC PCF Dynamic Policy Control (Rx).

4.55 Configurable MultiSIM Support for Sy/ESy

Introduced in: SAPC 1.13 EP2

4.55.1 Description of Impacts:

Configuration parameter `enableMultipleSubscriptionsToOcs` is introduced to enable or disable sending multiple subscriber identifiers to OCS.

When the MSISDN and IMSI come from Gx interface, or the GPSI and SUPI from N7 interface, and `enableMultipleSubscriptionsToOcs` configuration parameter value is `TRUE`, then the `Subscription-Id` AVP of SLR in Sy/ESy interface will include both IMSI and MSISDN.

For more information, refer to Integration with OCS for Monetary Spending Limit Reporting (Sy).

4.55.2 Capacity and Performance

No impact

4.55.3 Interface

No impact

4.55.4 Operation

New configuration parameter `enableMultipleSubscriptionsToOcs` is added below `AppConfig` class in the MOM.

4.56 Presence Reporting Area Support on N7 Interface

Introduced in: SAPC 1.14.0

4.56.1 Description of Impacts

The Presence Reporting Area (PRA) function enables the SAPC PCF to select areas where presence of the subscriber is reported. The change of presence state for an area is reported by the SMF. The SAPC PCF makes policy decisions based on the presence state and sends the policy decisions to the SMF.

For more information, refer to Access and Charging Control (N7).

4.56.2 Capacity and Performance

Impact in the traffic model: additional SM policy control update notification requests to inform the selected PRAs, and additional SM policy control update requests to report the presence states of PRAs.

Impact to memory: selecting multiple PRAs or PRAs with additional IDs, and storing the presence states for PRAs.

4.56.3 Interface

— Provisioning REST API

  • Added `additionalPraIds` attribute in `/profiles/presence-reporting-area/{profileId}` URI.

— N7 Interface

  • Support `PRA_CH`, `SAREA_CH`, and `SCELL_CH` values in `PolicyControlRequestTrigger` data structure.

  • Added PRA in `SupportedFeatures` data structure.

  • Added `praInfos` attribute in `SMPolicyDecision` data structure and `repPraInfos` attribute in `SmPolicyUpdateContextData` data structure.

4.56.4 Operation

— Added new values to EventTriggers in MoM, corresponding to policy control request triggers in N7:

- 210 for SAREA_CH
- 214 for SCELL_CH
- For PRA_CH, the existing 48 (CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT) value is reused

— Support the Presence Reporting Area Selection policy type over the N7 interface.

— Support the following policy tags over the N7 interface:

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

— Added the `AccessData.subscriber.locationInfo.presenceState["praId"]` policy tag.

For more information, refer to Configuration Guide for Access and Charging Control (N7).

4.57 SAPC PCF Supports NetLoc for Voice over New Radio

Introduced in: SAPC 1.14.0

4.57.1 Description of Impacts

The SAPC PCF supports to provide NetLoc function for Voice over New Radio (VoNR) calls.

The SAPC PCF supports failure handling of NetLoc function when PDU session does not support NetLoc.

The SAPC PCF supports NetLoc for IMS Emergency Services.

For more information, refer to Dynamic Policy Control (Rx) for SAPC PCF.

4.57.2 Capacity and Performance

No impact

4.57.3 Interface

The following changes are made to support failure handling of NetLoc:

- N7
  - Added the `netLocAccSupp` attribute in the `UeCampingRep` data structure of the `Npcf_SMPolicyControl_UpdateNotify` response.

4.57.4 Operation

No impact

4.58 Disable Notification of Bearer Events to the AF Updates

Introduced in: SAPC 1.14.0

4.58.1 Description of Impacts

The SAPC PCF supports disabling the notification of bearer Network Location Information events of to the AF.

For more information, refer to Dynamic Policy Control (Rx) for SAPC PCF.

4.58.2 Capacity and Performance

No impact

4.58.3 Interface

No impact

4.58.4 Operation

A new value ACCESS_NETWORK_INFO_REPORT is added to `disabledSpecificActions` attribute in the `PccConfig` class in the MOM.

4.59 Disable Subscriber Profile Access by APNs or DNNs

Introduced in: SAPC 1.14.0

4.59.1 Description of Impacts

To reduce signaling processing loads, the SAPC supports disabling subscriber profile access by APN or DNN. When the SAPC receives a request (or processes an internal reauthorization) dealing with the selected APN or DNN, the SAPC uses Subscriber Unknown profile instead of querying subscription information from internal or external database. This function affects Gx, Rx, and N7

traffic. For more information, refer to Subscription and Policy Management and Subscription and Policy Management for SAPC PCF.

4.59.2 Capacity and Performance

No impact

4.59.3 Interface

No impact

4.59.4 Operation

The APN or DNN to disable subscriber profile access is defined in new attribute `disableSubsProfileAccessIds` in the class `Apns` in the MOM.

For more information, refer to Configuration Guide for Subscription and Policies and Configuration Guide for SAPC PCF Subscription and Policies.

4.60 Extensions to Overload Protection of Priority Services for SAPC PCF: Access and Mobility Policy Control, and 5G Auto Provisioning

Introduced in: SAPC 1.14.0

4.60.1 Description of Impacts

When overloaded, the SAPC PCF:

- Rejects incoming `Npcf_AMPolicyControl_Create`, `_Update`, and `_Delete` messages to reduce its load answering with 503 Service Unavailable.
- Does not send the second `Nudr_DataRepository_Query` request to the UDR to query the sm-data again during 5G Auto Provisioning for N7 Session.

4.60.2 Capacity and Performance

No impact

4.60.3 Interface

No impact

4.60.4 Operation

The following measurements are added:

— NpcfAmCreateTooBusy

— NpcfAmUpdateTooBusy

— NpcfAmDeleteTooBusy

The following alarm is added:

— Policy Control, Number of Npcf_AMPolicyControl_Create Responses Sent Indicating Too Busy Reached

4.61 Addition of Location AVPs to 3GPP Sy Interface

Introduced in: SAPC 1.15.0

4.61.1 Description of Impacts

The 3GPP standard Sy interface is enhanced to support the subscriber location information in the SLR message to OCS. Whether the SAPC includes the subscriber location information in the SLR message depends on the configuration of attribute `locationInfoEnabled` per OCS profile.

4.61.2 Capacity and Performance

No impact

4.61.3 Interface

For 3GPP standard Sy interface, the following optional AVPs are introduced in the SLR message:

— `3GPP-SGSN-MCC-MNC`

— `3GPP-SGSN-Address`

— `3GPP-SGSN-IPv6-Address`

For provisioning REST API, optional attribute `locationInfoEnabled` is introduced in the OCS profile.

4.61.4 Operation

No impact

4.62 SAPC PCF Supports 2/4/5G Converged SMF

Introduced in: SAPC 1.15.0

4.62.1 Description of Impacts

The SAPC PCF supports to receive new 2G parameters or data types when subscribing UE to the 2G network through the converged SMF devices.

The SAPC PCF also supports to configure the PCC rules, and deliver authorized QoS information to the converged SMF devices for 2G accesses.

4.62.2 Capacity and Performance

No impact

4.62.3 Interface

For N7 interface, the following changes are introduced:

- Value `RAI_CH` is supported in `PolicyControlRequestTrigger` data structure.
- Value `GERA` is supported in `RatType` data type.
- New data type `SgsnAddress` is supported, attribute `sgsnAddr` is added in `ServingNfIdentity` data structure.
- New data type `GeraLocation` is supported, attribute `geraLocation` is added in `UserLocation` data structure.

4.62.4 Operation

A new attribute `enable2GEventTrigger` is introduced in class `PcfAppConfig` in the MOM.

For SAPC PCF, added support of the policy control request trigger `RAI_CH(12)`.

For SAPC PCF, added support of the policy tag `AccessData.subscriber.locationInfo.sgsnAddress`.

4.63 EBM for N7

Introduced in: SAPC 1.15.0

4.63.1 Description of Impacts

The EBM for N7 function provides EBM events related to the N7 interface. For more information, refer to Event-Based Monitoring.

4.63.2 Capacity and Performance

According to measurements, the impact of EBM for N7 on performance is the following:

When events for the N7 interface to be reporting through EBM are configured, the performance drop of the N7 traffic regarding the baseline is 9%.

4.63.3 Interface

With the introduction of EBM for N7, the following events can be sent through the EBM interface:

- `NPCF_SMPOLICY_CONTROL_CREATE`
- `NPCF_SMPOLICY_CONTROL_UPDATE`
- `NPCF_SMPOLICY_CONTROL_UPDATE_NOTIFY`
- `NPCF_SMPOLICY_CONTROL_DELETE`
- `DEFAULT_PDU_SESSION_QOS_ASSIGNED`
- `PCC_RULE_INSTALLED`
- `PCC_RULE_INSTALLATION_FAILURE`
- `PCC_RULE_REMOVED`

4.63.4 Operation

No impact

4.64 N+1 Geographical Redundancy in SAPC 1.15

Introduced in: SAPC 1.15.0

Disclaimer: N+1 Geographical Redundancy is a fully restricted feature. All N+1 related content has been included in official documentation in order to maintain a single documentation track. This feature cannot be enabled without proper approval.

4.64.1 Description of Impacts

N+1 Geographical Redundancy in SAPC 1.15.0 includes:

— Collision detection control mechanism for Fair Usage feature and for Sd protocol.

— Update subscriber Operator-Specific-Info by policies supported in N+1 Georgraphical Redundancy deployments.

4.64.2 Capacity and Performance

Minimum resources for the N+1 deployment in Cloud has been updated: The minimum number of vCPUs assigned to TP virtual machines is set to 4 vCPUs.

4.64.3 Interface

No impact

4.64.4 Operation

CDC attribute added in the following EDS:

— AccumulatedUsage

The following log events are added for N+1 Geographical Redundancy in SAPC 1.15.0:

— Collision Detection Control Failure Updating Accumulated Usage

The following log events are modified for N+1 Geographical Redundancy in SAPC 1.15.0:

— Received Usage

— Update Accumulated Usage Failed

— Collision Detection Control Failure Updating Session Data

The following alarm is added:

— Policy Control, Geographical Redundancy Subscriber Operator-Specific-Info Update Replication Failure

4.65 SAPC PCF Support for User Notifications by SOAP

Introduced in: SAPC 1.15.0

4.65.1 Description of Impacts

The SAPC PCF supports sending SOAP notifications to external systems as described in User Notifications.

4.65.2 Capacity and Performance

The request and response time for 5G traffic is not affected by the user notifications because the notification policies are evaluated after a request or response is sent.

The TPS of 5G traffic is affected because the policy evaluation and the handling of SOAP messages consumes some CPU time and network resources.

4.65.3 Interface

The SAPC PCF uses SOAP protocol to connect with the notification servers, same as SAPC PCRF.

4.65.4 Operation

The same configuration related to SOAP notifications for the SAPC PCRF also applies to the SAPC PCF.

For more information, refer to Configuration Guide for End User Notifications.

4.66 EDA Geographical Redundancy in 5G Auto Provisioning

Introduced in: SAPC 1.15.0

4.66.1 Description of Impacts

The SAPC PCF supports EDA active-active geographical redundancy in 5G auto provisioning. The SAPC sends SOAP notifications to one of the web service destinations in EDASOAP Web Service End Point following the round-robin algorithm. For more information, refer to 5G Auto Provisioning.

4.66.2 Capacity and Performance

No impact

4.66.3 Interface

No impact

4.66.4 Operation

In EDASOAP Web Service End Point, 2 web service destinations can be configured.

4.67 EBM for N7 Enhancement

Introduced in: SAPC 1.16.0

4.67.1 Description of Impacts

This enhancement adds more EBM events related to the N7 interface. For more information, refer to Event-Based Monitoring.

4.67.2 Capacity and Performance

According to measurements, the impact of the EBM for N7 Enhancement on performance is the following:

When events of the enhancement for the N7 interface to be reported through EBM are configured, the performance drop of the N7 traffic regarding the baseline is 7%.

4.67.3 Interface

With the introduction this enhancement, the following events can be sent through the EBM interface:

- USAGE_MONITORING_QUOTA_GRANTED
- USAGE_REPORTING_ACCUMULATED_USAGE
- USAGE_MONITORING_LIMIT_SURPASSED
- USAGE_MONITORING_ACCUMULATED_USAGE_RESET
- USAGE_MONITORING_SUBSCRIPTION_DATA
- PRESENCE_REPORTING_AREA_INFO_N7

4.67.4 Operation

No impact

4.68 AM (N15) and SM (N7) Joint Policy Evaluation

Introduced in: SAPC 1.16.0

4.68.1 Description of Impacts

The SAPC PCF supports joint policy evaluation for a subscriber based on the information from the bound N7 and N15 sessions.

For more information, refer to AM (N15) and SM (N7) Joint Policy Evaluation.

4.68.2 Capacity and Performance

Performance degradation is expected when the feature is enabled.

4.68.3 Interface

No impact

4.68.4 Operation

Added the following new attributes under **PcfConfig** > **PcfAppConfig** > **JointPolicyEvaluation=1**:

- `enableJointPolicyEvaluation`
- `subscribePRA`

Added the following policy tags for joint policy evaluation:

- `AccessData.bearer.all.accessPoint`
- `AccessData.bearer.all.accessType`
- `AccessData.bearer.all.ipCanType`
- `AccessData.subscriber.locationInfo.all.cellIdentity`
- `AccessData.subscriber.locationInfo.all.countryCode`
- `AccessData.subscriber.locationInfo.all.networkCode`
- `AccessData.subscriber.locationInfo.all.routingAreaCode`
- `AccessData.subscriber.locationInfo.all.timezone`
- `AccessData.subscriber.service["serviceName"].isAnyRunning`

— `AccessData.subscriber.service["serviceName"].media.type["mediaType"].isAnyRunning`

For more policy tags which can be used for joint policy evaluation, refer to Configuration Guide for AM (N15) and SM (N7) Joint Policy Evaluation.

4.69 SAPC PCF Supports Wi-Fi Calling

Introduced in: SAPC 1.16

4.69.1 Description of Impacts

The SAPC PCF supports Wi-Fi calling in following scenarios:

— The establishment of Voice over Wi-Fi (VoWiFi) calls

— The handover between VoWiFi and VoNR/VoLTE

— The Emergency Calls over Wi-Fi from authorized users

For more information, refer to Policy Control for Wi-Fi Calling.

4.69.2 Capacity and Performance

No impact

4.69.3 Interface

The following changes are introduced to N7 interface:

— In data types `SmPolicyContextData`, `SmPolicyUpdateContextData`, and `UeCampingRep`, added the following new values:

  • `accessType`: `NON_3GPP_ACCESS`

  • `ratType`: `WLAN`

— In data type `UserLocation`, added new attribute `n3gaLocation`.

For more information, refer to N7 Interface Description.

The following changes are introduced to Rx interface:

— In messages Rx AA-Answer (AAA) and Rx Re-Auth-Request (RAR), the following new values are added for SAPC PCF:

  • `[ AN-Trusted ]`: `UNTRUSTED (1)`

- `[ IP-CAN-Type ]: Non-3GPP-5GS (9)`
- `[ RAT-Type ]: WLAN (0)`

— In messages Rx Re-Auth-Request (RAR) and Rx Session-Termination-Answer (STA), the following AVPs are supported for SAPC PCF:

- `[ UE-Local-Ip-Address ]`
- `[ TCP-Source-Port ]`
- `[ UDP-Source-Port ]`

— In Rx Supported-Features, added the support of feature `NetLoc-Untrusted-WLAN` for SAPC PCF.

— In Mapping Table for IP-CAN Types and Access Types, added the non 3GPP access related mapping.

For more information, refer to Rx Interface Description.

The following changes are introduced to the EBM interface:

— Added new structure `EXTENDED_IPCAN_TYPE_INFO` in following events:

- RX_AAR_AAA_TRANSACTION
- RX_RAR_RAA_TRANSACTION

— Added new structure `UNTRUSTED_LOCATION_INFO_5G` in following events:

- RX_RAR_RAA_TRANSACTION
- RX_STR_STA_TRANSACTION
- NPCF_SMPOLICY_CONTROL_CREATE
- NPCF_SMPOLICY_CONTROL_UPDATE
- NPCF_SMPOLICY_CONTROL_DELETE

For more information, refer to Event-Based Monitoring.

4.69.4 Operation

The following changes are introduced to the policy tags for Access and Charging Control and Dynamic Policy Control:

— For policy tag `AccessData.bearer.accessType`, added value `WLAN (0)`

— For policy tag `AccessData.bearer.ipCanType`, added value `9: Non_3GPP_5GS`

— Added policy tag `AccessData.bearer.isAnTrusted`

For Wi-Fi calling specific policy tag `AccessData.bearer.handover`, add the following values for SAPC PCF:

— 3: Handover from Wi-Fi to EUTRA

— 4: Handover from EUTRA to Wi-Fi

— 5: Handover from Wi-Fi to NR

— 6: Handover from NR to Wi-Fi

4.70 SAPC PCF Support for Access Network Charging Identifier (AN-CID) Information

Introduced in: SAPC 1.16

4.70.1 Description of Impacts

The SAPC PCF supports providing Access Network Charging Identifier (AN-CID) Information from the SMF to the AF. The AN-CID information is used by the AF for charging correlation with session layer.

For more information, refer to Dynamic Policy Control (Rx) for SAPC PCF.

4.70.2 Capacity and Performance

The AN-CID is requested during the establishment of an AF session. When the SMF assigns the AN-CID for the dynamic PCC rules, the SMF reports the Access Network Charging Information as a new N7 Update message.

The activation of this function increases the number of messages exchanged between the SAPC PCF and other nodes in the network (for example, incoming N7 Update message reporting the Access Network Charging Information that triggers an outgoing Rx:RAR message towards the AF).

The additional memory for each PDU session is required to save specific parameters and values supported in this function.

4.70.3 Interface

The following attributes and values are supported over the N7 interface:

— The AN_CH_COR (28) value in the policyCtrlReqTriggers attribute in Npcf_SMPolicyControl_Create, Npcf_SMPolicyControl_Update, and Npcf_SMPolicyControl_UpdateNotify messages.

— The CH_ID value in the reqData attribute in Npcf_SMPolicyControl_UpdateNotify messages.

— The accNetChId attribute in Npcf_SMPolicyControl_Create messages.

— The accNetChIds attribute in Npcf_SMPolicyControl_Update messages.

The following parameters and values are supported over the Rx interface:

— The Access-Network-Charging-Identifier AVP (AVP code 502) in AAA and RAR messages.

— The CHARGING_CORRELATION_EXCHANGE (1) value of the Specific-Action AVP in AAR and RAR messages.

4.70.4 Operation

No impact

4.71 X-AF-Charging-Identifier

Introduced in: SAPC 1.16

4.71.1 Description of Impacts

The SAPC PCRF and the SAPC PCF support the X-AF-Charging-Identifier AVP optionally used by the AF to replace the service identifier and rating group of the charging information in dynamic PCC rules.

4.71.2 Capacity and Performance

No impact

4.71.3 Interface

Rx interface:

— Added the optional AVP X-AF-Charging-Identifier (AVP code 2299, Vendor-Id 28357) to AAR messages.

4.71.4 Operation

No impact

4.72 Split Brain Mitigation

Introduced in: SAPC 1.16

4.72.1 Description of Impacts

The SAPC provides the split brain mitigation tool to prevent the inconsistency that could be created in the database due to nodes not able to communicate as a consequence of major media outage in an active-active deployment.

This feature works only in Active-Active Geographical Redundancy deployments. For more information, see Active-Active Geographical Redundancy.

4.72.2 Interface

With this tool active, in case of a split-brain, we assure Diameter Gx traffic towards the non-preferred node in every 5 minutes (or configurable revalidation timeout).

4.72.3 Operation

This feature is disabled by default. It can be enabled or modified by the configuration of Flexible Output Policies. New Entity Data Target `SplitBrainMitigation` is provided for this. For more details, seeActive-Active Geographical Redundancy User Guide.

4.73 Active-Active Geographical Redundancy for SAPC PCF

Introduced in: SAPC 1.17

4.73.1 Description of Impacts

Geographical Redundancy deployment in active-active mode is implemented for SAPC PCF, where both SAPC peers are active and can handle incoming traffics simultaneously. Each SAPC keeps the state of the mated peer, and is ready to take over the incoming traffics when the mated peer is out of service. For more information, refer to Active-Active Geographical Redundancy.

The deletion of sessions through session-handler tool also supports the Geographical Redundancy deployment. When both SAPC peers are in Distributed state, the delete operation of session-handler uses session mastership as one of the criteria to remove specific sessions. For more information of session-handler, refer to SAPC Troubleshooting Guide.

4.73.2 Capacity and Performance

No impact.

4.73.3 Interface

For N7 interface, added HTTP header `3gpp-Sbi-Binding` in following request/response:

— `Npcf_SMPolicyControl_Create Response`

— `Npcf_SMPolicyControl_Update Response`

— `Npcf_SMPolicyControl_UpdateNotify Request`

For N15 interface, added HTTP header `3gpp-Sbi-Binding` in following request/response:

— `Npcf_AMPolicyControl_Create Response`

— `Npcf_AMPolicyControl_Update Response`

— `Npcf_AMPolicyControl_UpdateNotify Request`

For Nudr interface, added HTTP header `3gpp-Sbi-Binding` in following request/response:

— `Nudr_DataRepository_Subscribe Request`

— `Nudr_DataRepository_Notify Response`

Note: The CCDM only supports the `3gpp-Sbi-Binding` header in `Nudr_DataRepository_Subscribe Request`.

For Nbsf interface, introduced the following changes:

— `Nbsf_Management_Update` operation is supported.

— For `Nbsf_Management_Register Request`, added value `BindingUpdate` to the `suppFeat` attribute.

— For `Nbsf_Management_Register Request`, added attributes `bindLevel` and `pcfSetId`.

For Nnrf interface, introduced the following changes:

— Added attribute `nfSetIdList` in the `NFProfile`.

— Supported to register custom service name `npcf-notify-nudr` to NRF.

For HTTP/2 message relay between two SAPC peers, introduced the support of following messages over Replication Channel:

— `Npcf_SMPolicyControl_UpdateNotify`

— `Npcf_AMPolicyControl_UpdateNotify`

— `Nbsf_Management_Register`

— `Nbsf_Management_Update`

— `Nbsf_Management_Deregister`

4.73.4 Operation

The following changes are introduced to the MOM:

— Added new attribute `pcfNfSetIdList` in the `PcfAppConfig` class to configure the NF Set information of the SAPC PCF peers.

  For more information, refer to Configuration Guide for Interaction with NRF.

— Added new class `PcfGeoRedConfig` to contain the PCF Geographical Redundancy related configuration, with attributes `enableSessionStickiness` and `enableConnectionRedundancy`.

  For more information, refer to Active-Active Geographical Redundancy.

— Added new attribute `enableTLSClientAuthenticationRelay` in the `PcfSecurity` class to control the TLS client authentication of the relayed HTTP2 messages.

The following measures are introduced to the measurements:

— New measure `NpcfSmUpdateNotifyRelayed` in measure group `policyControlFunctionNpcfSmMeasuresGroup`.

— New measure `NpcfAmUpdateNotifyRelayed` in measure group `policyControlFunctionNpcfAmMeasuresGroup`.

— New measures in measure group `PolicyControlFunctionNbsfMeasuresGroup`:

  • `NbsfRegisterRelayed`

  • `NbsfDeregisterRelayed`

  • `NbsfUpdateRelayed`

  • `NbsfUpdateRequests`

- NbsfUpdateFailed
- NbsfUpdateSuccess

The following changes are introduced to the logging events:

— Added new logging event HTTP/2 message relayed.

— Added Update request type and PATCH method in Additional Info for following logging events:

- Error sending HTTP Request
- HTTP Response Received
- HTTP Request Sent
- Timeout Receiving HTTP Response
- Unsuccessful HTTP Response Received

For alarm GeographicalRedundancyUnableToReachPeer, source ManagedElement=1,PolicyControlFunction=1,GeoRedManager=1,RelayChannel,PL=<PL-X> is introduced for HTTP/2 message relay in Active-Active Geographical Redundancy.

4.74 SCP Traffic Separation

Introduced in: SAPC 1.17

4.74.1 Description of Impacts

For multiple traffic types to SCP through different traffic VIPs, the SAPC PCF supports to handle them separately by setting up individual connection pools for each traffic VIP. For example, the SAPC PCF can establish one connection pool for N7 traffic VIP and another connection pool for N15 traffic VIP. To same SCP, the HTTP requests are distributed by traffic VIPs in corresponding connection pools respectively.

4.74.2 Capacity and Performance

No impact

4.74.3 Interface

No impact

4.74.4 Operation

For alarm `ConnectionToSCPFailed`, introduced the following changes to the alarm attributes:

— Source: added the value `peerNodeId=<nfInstanceID:SourceIp>`, removed the value `SCP=<fqdn>`.

— Additional Text: value `<nfInstanceID>` is changed to `<nfInstanceID:SourceIp>`.

For log event *PCF PeerNode status change*, introduced the following changes to the Additional Info:

— PeerNode: added the value `SCPNodeID:SourceIp`.

— PeerNodeType: added the value `SCP`.

4.75 5G Auto Provisioning Enhancements in SAPC 1.17

Introduced in: SAPC 1.17.0

4.75.1 Description of Impacts

The following functions are added in the enhancement of 5G Auto Provisioning:

— More messages such as IMEI, DNN, and user location information can be sent to the EDA 2. The notification templates can be selected depending on conditions of a policy.

— If a notification for a subscriber has been sent to the EDA 2, the 5G Auto Provisioning can be suppressed by a period of time.

For more information, refer to 5G Auto Provisioning.

4.75.2 Capacity and Performance

No impact

4.75.3 Interface

No impact

4.75.4 Operation

A new attribute `PcfAutoProvisionSuppressionDuration` is added under class `PcfAppConfig`.

The 5G Autoprovisioning policy type is added.

4.76 SAPC PCF Resubscription to UDR before Expiration

Introduced in: SAPC 1.17

4.76.1 Description of Impacts

The subscription to UDR notifications may expire in the UDR while the PCF is not aware of this expiration.As a result, when a N7/N15 session exists longer than expiration time in the UDR, no notification message is sent to the PCF from the UDR.

Note: In CCDM, the `maximum-subscription-duration` parameter can be set up to 14 days.

The SAPC PCF provides a solution to resubscribe to the UDR after a configured duration. This behavior is disabled by default. If configured, a session reauthorization and policy evaluation is triggered when the configured timer is reached. This reauthorization triggers a new UDR subscription message.

4.76.2 Capacity and Performance

No impact

4.76.3 Interface

No impact

4.76.4 Operation

The functionality of the "SAPC PCF resubscription to UDR before expiration" can be enabled by adding a new parameter in the CFG of the processes. This parameter sets the duration of the UDR subscription, after which SAPC PCF should consider the subscription as expired and send a new subscription request towards UDR.

4.77 Load Control Based on Load Control Information(LCI)

Introduced in: SAPC 1.18

4.77.1 Description of Impacts

The load control function allows for better balancing of load across the NF Service Producers. The load control enables the SAPC PCF to signal its load

information to the PCF Service Consumers via the NRF or directly to the PCF Service Consumer.

For more information, refer to Load Control User Guide.

4.77.2 Capacity and Performance

No impact

4.77.3 Interface

For N7 interface, added HTTP header `3gpp-Sbi-Lci` in the following request/response:

— `Npcf_SMPolicyControl_Create` Response

— `Npcf_SMPolicyControl_Update` Response

— `Npcf_SMPolicyControl_UpdateNotify - Modification` Request

— `Npcf_SMPolicyControl_UpdateNotify - Termination` Request

— `Npcf_SMPolicyControl_Delete` Response

For N15 (AMPC) interface, added HTTP header `3gpp-Sbi-Lci` in the following request/response:

— `Npcf_AMPolicyControl_Create` Response

— `Npcf_AMPolicyControl_Update` Response

— `Npcf_AMPolicyControl_UpdateNotify` Request

— `Npcf_AMPolicyControl_Delete` Response

For Nnrf interface, added `lcHSupportInd` in NFProfile data structure.

4.77.4 Operation

The following changes are done to MOM:

— Added a new class `LoadReportingConfig` under class `PcfAppConfig`.

— Added the following new tags in SAPC PCF registration profile:

  • {LCH_SUPPORT}

  • {LOAD}

- {LOAD_TIMESTAMP}

A new logging event is introduced: Load reporting in LCI header sent.

4.78 Application Detection and Control (ADC) over N7 Interface

Introduced in: SAPC 1.18

4.78.1 Description of Impacts

The support of Application Detection and Control (ADC) over N7 interface provides the following functions:

— The SAPC PCF selects PCC rules for application detection and have the selected PCC rules installed in the SMF.

— The SAPC PCF receives report of status change from the SMF when the SMF detects application traffic start or stop.

— The SAPC PCF makes PCC decisions based on the report of detected application traffic status.

This function also supports redirecting the detected applications to another destination, or muting notifications to the SAPC PCF for specific applications. For more information, refer to Application Detection and Control Based on PCC rules (N7).

4.78.2 Capacity and Performance

No impact

4.78.3 Interface

The following attributes and values are supported over the N7 interface:

— The `redirectinfo` and `muteNotif` attributes in `TrafficControlData` type.

— The `appId` attribute in `PccRule` type.

— The `appDetectionInfos` attribute in `SmPolicyUpdateContextData` type.

— The `APP_STA` and `APP_STO` value in `PolicyControlRequestTrigger` type.

— The `APP_ID_ERR` and `MISS_REDI_SER_ADDR` values in `FailureCode` type.

Apart from the above, feature number 4 (ADC) is supported in `SupportedFeatures` type. Error code `404 Not Found` with HTTP cause

POLICY_ASSOCIATION_NOT_FOUND is supported in Npcf_SMPolicyControl_Update response and Npcf_SMPolicyControl_Delete response. For more information, refer to N7 Interface Description.

The following event is updated to be sent through the EBM interface:

— Added new structure PCC_ADC_RULE_INFORMATION into the PCC_RULE_INSTALLED event.

For more information, refer to Event-Based Monitoring.

4.78.4 Operation

The following changes are done to MOM:

— Added `adcSupport` attribute under class `PcfPeerNode`.

For more information, refer to Configuration Guide for ADC Based on PCC Rules (N7).

The following policy tag is added for ADC information used by joint policy evaluation:

— `AccessData.tdfApp["id"].isAnyStarted`

For more information, refer to Configuration Guide for Joint Policy Evaluation on AM (N15) and SM (N7).

The following measures are introduced to measure group "policyControlFunctionNpcfSmMeasuresGroup":

— NpcfSmAdcStartEvents

— NpcfSmAdcStopEvents

For more information, refer to Measurements.

4.79 Enhancement of SAPC PCF Support for Emergency Services in SAPC 1.19

Introduced in: SAPC 1.19.0

4.79.1 Description of Impacts

The SAPC PCF supports IMS emergency services for roaming subscribers.

In case that the AF has no IMS-level roaming interfaces, the AF might request the SAPC PCF to provide the EPC-level identities (MSISDN, IMSI, or IMEI(SV)) as

part of the establishment of an IMS emergency registration or an IMS emergency session establishment.

For information on IMS emergency services, see Emergency and Multimedia Priority Services.

4.79.2 Capacity and Performance

EPC-Level identities request is supported at IMS emergency registration or an IMS emergency session establishment.

Impact in the traffic model:

— If the EPC-Level identities information is requested at IMS emergency registration, the additional Rx diameter session other than the one for IMS emergency session will be established. 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.

4.79.3 Interface

On Rx interface:

— Support the `AF-Requested-Data` AVP in AAR.

— Support the `Subscription-Id` and `User-Equipment-Info` AVPs in AAA.

4.79.4 Operation

No impact

4.80 SAPC PCF Support of PLMN change notification to the AF

Introduced in: SAPC 1.19.0

4.80.1 Description of Impacts

The Public Land Mobile Network (PLMN) Information Change Notification is a mechanism to report the PLMN where the UE is located once the PLMN Id becomes available or updated, to the AF which previously subscribed to this bearer event.

For details, see the *PLMN Information Change Notification* function description and traffic case in Dynamic Policy Control (Rx) for SAPC PCF.

4.80.2 Capacity and Performance

— PLMN change notification is supported at IMS SIP registration or IMS SIP call negotiation.

  Impact in the traffic model:

  - It increases the frequency of N7 and Rx operations to report PLMN changes to the AF node.
  - If the PLMN change notification is required at IMS SIP registration, the additional Rx diameter session other than the one for IMS SIP call will be established. 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.

4.80.3 Interface

— On N7 interface:

  - Added `PLMN_CH` policy control request trigger.
  - Added `servingNetwork` attribute in UeCampingRep data structure in Npcf_SMPolicyControl_UpdateNotify response.

— On Rx interface:

  - Support `PLMNInfo` in `Supported-Feature` AVP.
  - Support `PLMN_CHANGE` in `Specific-Action` AVP.

4.80.4 Operation

For Event-Based Monitoring:

— PLMN_CH is added in POLICY_CONTROL_TRIGGERS structure for NPCF_SMPOLICY_CONTROL_CREATE, NPCF_SMPOLICY_CONTROL_UPDATE and NPCF_SMPOLICY_CONTROL_UPDATE_NOTIFY events.

— PLMN_CH is added in RECEIVED_POLICY_CONTROL_TRIGGERS structure for NPCF_SMPOLICY_CONTROL_UPDATE event.

In Managed Object Model (MOM):

— The PLMN_CHANGE value in `disabledSpecificActions` is also applicable for the SAPC PCF.

— The value 4 PLMN_CHANGE in `EventTriggers` is also applicable for the SAPC PCF.

4.81 SAPC PCF Support for SIP Forking

Introduced in: SAPC 1.19.0

4.81.1 Description of Impacts

The SAPC PCF supports voice for SIP forking. This function allows the IMS network to attempt simultaneously the establishment of the application session in multiple destinations where the subscriber might reach.

For more information, see Dynamic Policy Control (Rx) for SAPC PCF.

4.81.2 Capacity and Performance

No impact

4.81.3 Interface

On Rx interface, the SAPC PCF supports `SIP-Forking-Indication` AVP in AAR.

4.81.4 Operation

No impact

4.82 SAPC PCF Integration with OCS, for AM or UE Policy Control

Introduced in: SAPC 1.19.0

4.82.1 Description of Impacts

The SAPC PCF performs Access and Mobility (AM) Policy Control and UE Policy Control based on the information received from the Online Charging System (OCS). Both Sy and Esy interfaces are supported.

During the establishment and modification of AM policy association or UE policy association, the SAPC PCF determines whether information from the OCS is needed to calculate the data to send to the AMF. If it is so, the SAPC PCF first selects the OCS, then sends a request to the selected one and uses the received information, together with the subscriber data retrieved from the UDR, to decide the data to send to the AMF.

For more information, see Integration with OCS for Monetary Spending Limit Reporting (Sy).

4.82.2 Capacity and Performance

AMF KPI performance drops ~2% because of additional tasks performed for the Npcf_AMPolicyControl_Create, Update, and Delete operations.

4.82.3 Interface

The SAPC PCF handles the Sy or Esy messages by binding the Sy or Esy session with the N15 session from the AMF.

`Subscription-Id` AVP to interact with the OCS is obtained by extracting IMSI or MSISDN from SUPI or GPSI value received N15 requests.

4.82.4 Operation

The operation for N15 is the same as N7.

4.83 Multiple DNNs

Introduced in: SAPC 1.19.0

4.83.1 Description of Impacts

The SAPC PCF supports sending multiple-DNN session rules to the SMF in PDU session establishment or modification. Each multiple-DNN session rule consists of service URLs, service DNN, and service S-NSSAI. For more information, see Access and Charging Control (N7).

4.83.2 Capacity and Performance

No impact

4.83.3 Interface

-Provisioning REST API

The following URIs are added:

— `/profiles/multiple-dnn-profile`

— `/profiles/multiple-dnn-profile/{profileId}`

The `multipleDnnProfileIds` attribute under `/dataplans/{dataplanId}/static-qualification` is supported.

4.83.4 Operation

No impact

4.84 Indirect Communication (Option C) with delegated reselection

Introduced in: SAPC 1.19.0

4.84.1 Description of Impacts

When the Indirect Communication (Option C) with delegated reselection is enabled, the SAPC PCF delegates SCP to reselect GeoRed deployed NFs (such as UDRs and BSF), by including the available factors in the request towards SCP. For more information, see Indirect Communication through SCP.

4.84.2 Capacity and Performance

This feature has impacts on memory and CPU load. Reading or Writing binding information costs extra resource. However, providing binding information is optional. The higher ratio of such information, the higher negative impact on the SAPC PCF overall characteristics.

4.84.3 Interface

For Nbsf interface:

— Added HTTP header `3gpp-Sbi-Routing-Binding` or `3gpp-Sbi-Discovery` in following requests:

  - Nbsf_Management_Register
  - Nbsf_Management_Update
  - Nbsf_Management_Deregister

For N36 interface:

— Added HTTP header `3gpp-Sbi-Routing-Binding` or `3gpp-Sbi-Discovery` in following requests:

  - Nudr_DataRepository_Query
  - Nudr_DataRepository_Update
  - Nudr_DataRepository_Subscribe
  - Nudr_DataRepository_UnSubscribe

4.84.4 Operation

The following changes are done to MOM:

— Added attribute `enableDelegatedReselection` under class `PcfNetwork`.

— Added attribute `scpDiscoveryHSupportInd` under class `PcfNetwork`.

For more information, refer to Configuration Guide for Indirect Communication through SCP.

4.85 Quota Rollover for SAPC PCF SPR Mode

Introduced in: SAPC 1.19.0

4.85.1 Description of Impacts

The Quota Rollover function enables users to spend the data not used at the end of the current period during the next one. The SAPC computes rollover data dynamically at the beginning of next billing cycle. Thus, during the next billing cycle the data usage limit for a given user would be the data usage limit entitled in the subscription plus the rollover data from previous period. Note that unused data are only rollover to next period, but not to subsequent ones.

The Quota Rollover function only applies for the SAPC PCF SPR mode.

For more information, refer to Usage Monitoring Control with SPR (N7).

4.85.2 Capacity and Performance

No impact

4.85.3 Interface

Provisioning REST API:

— support the following attributes under the `/subscribers/{subscriberId}/usage-limits` and `/dataplans/{dataplanId}/usage-limits` URIs:

  • `useRolloverFirst`

  • `rolloverLimit`

— support the following attributes under the `/subscribers/{subscriberId}/usage-accumulators` and `/shared-dataplans/{sharedDataplanId}/usage-accumulators` URIs:

  • `useRolloverFirst`

- `rolloverFromPreviousPeriod`
- `rolloverAccumulated`

4.85.4 Operation

— The following policy tags are supported for the SAPC PCF:

- `AccessData.subscriber.accumulatedUsage.group["groupName"].isRolloverSurpassed`
- `AccessData.subscriber.accumulatedUsage.group["groupName"].currentRollover`
- `AccessData.subscriber.accumulatedUsage.group["groupName"].currentRolloverPercentage`
- `AccessData.subscriber.accumulatedUsage.group["groupName"].rolloverFromPreviousPeriod`

— The following Logging Events are supported for the SAPC PCF:

- Rollover Limit Surpassed
- Usage Limit Surpassed
- Reset of Accumulated Usage Data

— The following measurements are supported for the SAPC PCF:

- usageLimitSurpassed

4.86 Refillable Dataplans for SAPC PCF SPR Mode

Introduced in: SAPC 1.19.0

4.86.1 Description of Impacts

The SAPC PCF enables the operator to activate automatically multiple instances with the same volume or time limits in a billing cycle for postpaid subscriptions. This is enabled by defining instances contracted for the subscriber groups associated with the subscribers. The subscribers can receive notifications on the use of the instances and are charged by the number of instances that they have started at the end of the billing cycle. Adding, changing or removing `startDate` refills the dataplan by resetting the number of `instancesContracted`.

The Refillable Dataplans function only applies for the SAPC PCF SPR mode.

For more information, refer to Usage Monitoring Control with SPR (N7).

4.86.2 Capacity and Performance

No impact

4.86.3 Interface

Provisioning REST API:

— Added `instancesContracted` attribute under the dataplan

— Added `instanceStarted` attribute under the usageAccumulators

4.86.4 Operation

The following policy tags are supported for the SAPC PCF:

— `AccessData.subscriber.accumulatedUsage.group["groupName"].currentInstance`

— `AccessData.subscriber.accumulatedUsage.group["groupName"].isInstanceAvailable`

— `AccessData.subscriber.accumulatedUsage.group["groupName"].newInstanceStart`

— `AccessData.subscriber.accumulatedUsage.group["groupName"].instanceStarted`

— `AccessData.subscriber.accumulatedUsage.group["groupName"].instanceRemained`

4.87 SAPC PCF Retransmission to UDR when Subscription Fails

Introduced in: SAPC 1.19.0

4.87.1 Description of Impacts

When the subscription to UDR notification is failed during the session creation, modification, or policy evaluation triggered reauthorization (such as ToD), the SAPC PCF may reattempt subscription according to configured times and intervals. The configuration is disabled by default.

For details of configuration, refer to System Administrator Guide.

4.87.2 Capacity and Performance

When retransmission is triggered, extra signaling between UDR and the SAPC PCF is needed, which will have minor impact on both performance and memory.

4.87.3 Interface

No impact

4.87.4 Operation

No impact

4.88 Network Location Information (NetLoc) Request Based on Dynamic PCC Rule of AF Signalling

Introduced in:SAPC 1.19.1

4.88.1 Description of Impacts

This function enables the SAPC PCRF and SAPC PCF to be requested and to report the Network Location Information based on the dynamic PCC rule of AF Signalling.

This is an Ericsson proprietary solution to request Access Network Information reporting for SMS over IP feature.

For more information, see Dynamic Policy Control (Rx) and Dynamic Policy Control (Rx) for SAPC PCF.

4.88.2 Capacity and Performance

This increases the frequency of Gx or N7 operations to report NetLoc information to the AF node.

If the AF session is not created at IMS SIP registration, a new AF session is then established at SIP MESSAGE for the "Access Network Information" reporting specifically, this AF session is terminated immediately upon retrieving the information. Therefore, the number of active Rx diameter sessions is increased, which impacts the dimensioning of the node and the capacity license of dynamic policy control.

4.88.3 Interface

No impact

4.88.4 Operation

No impact

4.89 EPS Fallback Notification

Introduced in: SAPC 1.20.0

4.89.1 Description of Impacts

EPS Fallback Notification enables the SAPC PCF to report the event to the AF when a QoS Flow with 5QI=1 is rejected due to EPS Fallback to the AF. If the AF successfully subscribes to the EPS fallback notification for IMS voice service, the SAPC PCF would send the EPS fallback indication to the AF when it receives from the SMF.

4.89.2 Capacity and Performance

5G Voice traffic profile is modified, when EPS-Fallback is activated.

The frequency of N7 update is increased: additional Update operation in N7 interface is used to report EPS-Fallback event.

4.89.3 Interface

The following changes are done to the N7 interface:

— Added 35 (EPSFallbackReport) in `SupportedFeatures` data structure.

— Added `EPS_FALLBACK (17)` in `PolicyControlRequestTrigger` data structure.

— Added `EPS_FALLBACK` for `reqData` in `RequestedRuleData` data structure.

The following changes are done to the Rx interface:

— Added `EPS_FALLBACK (17)` value in the `Specific-Action AVP` in Rx AAR messages.

— Added `Supported-Features AVP` instance with `Feature-List-ID = 2`, to support `EPSFallbackReport`(bit 8) for only SAPC PCF.

4.89.4 Operation

In Managed Object Model (`MOM`):

— `EPS_FALLBACK_REPORT` is added to `disabledSpecificActions` attribute in the `PccConfig` class.

For Event-Based Monitoring:

— EPS_FALLBACK is added in POLICY_CONTROL_TRIGGERS and RECEIVED_POLICY_CONTROL_TRIGGERS structure for NPCF_SMPOLICY_CONTROL_UPDATE and NPCF_SMPOLICY_CONTROL_UPDATE_NOTIFY events.

— EPS_FALLBACK (17) is added in SPECIFIC_ACTION structure for RX_AAR_AAA_TRANSACTION and RX_RAR_RAA_TRANSACTION events.

— EPS_FALLBACK (4) is added in REQUESTED_RULE_DATA_TYPES under PCC_RULE_INSTALLED events.

For System Administrator Guide:

— The enable_non_commercial_supported_feature_rx parameter is added to enable or disable the SAPC PCF to send the non-commercial supported-feature to the AF.

4.90 Analytics REST API Enhancement

Introduced in: SAPC 1.20.0

4.90.1 Description of Impacts

The Get MSISDN and Get Subscriber Info are supported by the SAPC PCF.

The Operator can query MSISDN, using IPv4 address or IPv6 prefix, to obtain an MSISDN list.

The Operator can query subscriber information using a subscriber ID, and the retrieved subscriber information contains the following attributes:

— subscriberId

— ongoingSession

— closedSession (returned when enableSessionInfoPublication is set to "true")

— usageAccumulators

4.90.2 Capacity and Performance

No Impact

4.90.3 Interface

The following Analytics Rest APIs are supported in SAPC PCF.

For Get MSISDN:

— /sessions/{ipaddr}/msisdn-list

For Get Subscriber Info:

— /subscribers/{subscriberId}/subscriber-info

4.90.4 Operation

No impact

4.91 RPS for eth1 softIRQs Distribution

Introduced in: SAPC 1.20.0

4.91.1 Description of Impacts

To avoid overloading on one specific vCPU, RPS, which is disabled by default, can be enabled to distribute eth1 softIRQs to other vCPUs.

4.91.2 Capacity and Performance

Around 6% performance drop in TPS is observed when RPS function is enabled.

4.91.3 Interface

No Impact

4.91.4 Operation

For details, see section *Eth1 softIRQs Handling Causes Much Higher Load on One Specific vCPU than Others* in SAPC Advanced Troubleshooting Guideline.