Oracle® Communications

Policy Management
Network Impact Report

Release 12.6.1

F45503-02

April 2022

Oracle Communication Policy Management Network Impact Report

Table of Contents

Figures

Tables

1. INTRODUCTION

1.1 Purpose and Scope

This document highlights the changes in Oracle Communication Policy Management Release 12.6.1 that may have impact on your network, and should be considered during planning for this release implementation.

1.1 Disclaimers

This document summarizes Oracle Communication Policy Management Release 12.6.1 new and enhancement features as compared to previous release of 12.5.x/12.6.0 and the operations impacts of these features, at a high level.

NOTE: Feature implementations may change slightly during product test.

1.2 Glossary

This section lists terms and acronyms specific to this document.

Table 1: Acronyms

Acronym	Definitions
3GPP	Third-Generation Partnership Project
AAA	Authorize-Authenticate-Answer
AAR	Authorize-Authenticate-Request
ADC	Application Detection and Control
AF	Application Function
AMBR	Aggregate Maximum Bit Rate
ARP	Allocation Retention Priority
AVP	Attribute Value Pair
BSS	Business Support System
CALEA	Communications Assistance for Law Enforcement Act.
CCA	Credit-Control-Answer (CC-Answer)
CCR	Credit-Control-Request (CC-Request)
CMP	Configuration Management Platform
CSCF	Call Session Control Function
DCC	Diameter Credit Control
DPI	Deep Packet Inspection
DRA	Diameter Routing Agent
DSR	Diameter Signaling Router
FRS	Feature Requirements Specification
GBR	Guaranteed Bit Rate
G8, G9	Refers to the generation of HP server hardware.
GUI	Graphical User Interface

Acronym	Definitions
HA	High Availability
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HW	Hardware
IE	Internet Explorer
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LI	Lawful Intercept
LIMF	Lawful Intercept Mediation Function
LVM	Logical Volume Manager
MA	Management Agent
MCD	Media Component Description
MP	Message Processor
MPE	Oracle Multimedia Policy Engine
MPE-R	Oracle Multimedia Policy Engine – Routing Mode
MPE-S	Oracle Multimedia Policy Engine – Serving Mode
MRA	Oracle Multiprotocol Routing Agent
MS	Mediation Server
NFV-MANO	Network Function Virtualization Management and Orchestration
NFVO	Network Functions Virtualization Orchestrator
NOAM	Network OAM
NW-CMP	Network-Level Configuration Management Platform
OAM	Operations Administration Maintenance
OCS	Online Charging Service
OM	Operational Measurement
OSSI	Operation Support System Interface
PCC	Policy and Charging Control
PCD	Policy Connection Director
PCEF	Policy and Charging Enforcement Function (GGSN, PGW, DPI)

Acronym	Definitions
PCRF	Policy Control Resource Function (Oracle MPE)
P-CSCF	Proxy CSCF
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PNR	Push-Notification-Request
PUR	Profile-Update-Request
QCI	QoS Class Identifier
QoS	Quality of Service
RAR	Re-Auth-Request (RA-Request) SUPL
REST	Representational State Transfer
ROB	Release of Bearer
S-CMP	Site-Level Configuration Management Platform
S-CSCF	Serving CSCF
SGW	Serving Gateway
Sh	Diameter Sh Interface
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SNR	Subscribe-Notification-Request
SPR	Subscriber Profile Repository
STA	Session-Termination-Answer
STR	Session-Termination-Request
SRA	Successful Resource Allocation
TDF	Traffic Detection Function
TPS	Transactions Per Second
UD	Upgrade Director
UDR	User Data Repository
UE	User Equipment
UM	Upgrade Manager
UMCH	Usage Monitoring Congestion Handling
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
VO	Verification Office
XML	Extensible Markup Language

2. OVERVIEW OF POLICY MANAGEMENT RELEASE 12.6.1 FEATURES

The following enhancement is added in Policy Management Release 12.6.1:

KPI_DASHBOARD Enhancement-ER 33960815

This enhancement reduces the loading duration of the KPI Dashboard of CMP GUI installed in Virtual environment.

In the previous releases, the KPI dashboard used to take several minutes to load for a larger customer deployment (with multiple MPE and MRAs), which has been reduced to less than a minute in this release. As per the latest testing, with 50+ MPE-MRA nodes in Virtualized environment, the KPI dashboard loading time is just 30 seconds.

2.1 Policy Management Hardware Requirements

2.1.1 Supported Hardware

The Policy Management Release 12.6.1 software can be deployed on the hardware that was previously supported under Release 12.4.x/12.5.x/12.6.0:

- Compatible with HP Gen-8 and Gen-9 Rack Mount Server (RMS) and C-class Servers
- HP 6120XG and HP 6125XLG enclosure switches.

NOTE: HP Gen-6 and Gen-7 servers are NOT supported.

2.2 Policy Management Software Changes

2.2.1 Software Components

Components	Releases
Policy Management	**12.6.1.0.0_19.1.0**
TPD 64 Bit	7.8.2
COMCOL	6.5
PM&C	6.6
TVoE	3.5.0
HP Firmware FUP	2.2.11 (Minimum) 2.2.12 (Current)

2.2.2 UDR and SPR Product Compatibility

Products	Releases	Compatibility
Oracle Communication UDR*	12.1 or higher	MPE via Sh interface and CMP via RESTful API. Use of Profile V2, Profile V3, and Profile V4 schemas.

***NOTE:** Policy R12.4 does not support Oracle SDM SPR Release 9.3.1

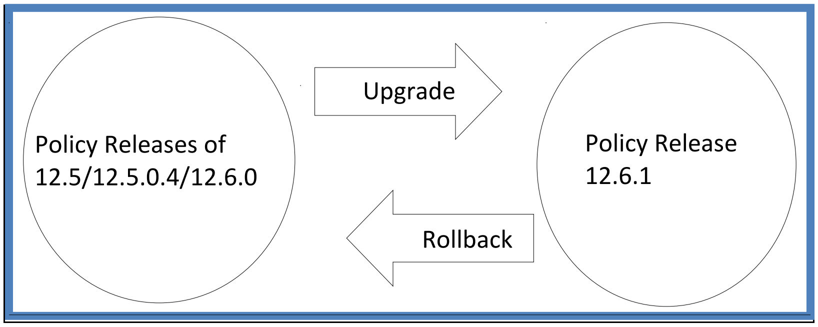
2.3 Policy Management Software Upgrade/Backout Overview

While performing the Policy software upgrade/rollback (backout) procedures, it is expected that the CMP clusters, MRA clusters, and MPE clusters are running different software releases.

2.3.1 Supported Software Upgrade/Rollback (Backout) Paths for Release 12.6.1

Figure 1 shows the supported upgrade Path for Release 12.6.1

Figure 1 Supportd Upgrade Path



As with the past releases, both Georedundant and Non-georedundant Policy deployments have separate Policy software upgrade/rollback (backout) procedures.

The system must be on release 12.5 or 12.5.0.4/12.6.0 prior to upgrading to this release (12.6.1). This applies to wireless line.

12.6.1 Upgrade Paths

- Policy Management 12.6.0 (full ISO) to 12.6.1 (full ISO) (Major Path)
- Policy Management 12.5.0.4 (patch ISO) to 12.6.1 (full ISO) (Minor Path)

• Policy Management 12.5.0 (full ISO) to 12.6.1 (full ISO) (Major Path)

NOTE:
• If the official upgrade paths mentioned in the release documents of each supported version is not followed, please contact Oracle Support before upgrading to 12.6.1. (Refer to individual patch release document to see the supported upgrade paths)
• 12.6.0 to 12.6.1 upgrade is only applicable for Bare Metal deployments

2.3.2 Mixed Version Policy Management System Expectations

The system that is running 12.5.0/12.5.0.4/12.6.0 mixed configuration supports the performance and capacity of 12.5.0/12.5.0.4/12.6.0 respectively. The mixed version Policy Management configuration supports Release 12.5.0/12.5.0.4/12.6.0 features respectively.

In the mixed version Policy Management configuration, Release 12.6.1 CMP has these general limitations:

- Policy rules should not be changed while running in a mixed version environment. If it is necessary to make changes to the policy rules while running in a mixed version environment, changes that do not utilize new conditions and actions for the release can be installed. However, these rules should be reviewed by you and Oracle before deployment to verify that the policies do not use new conditions or actions.
- The support for configuration of MPE and MRA servers is limited to parameters that are available in the previous version. Specifically:
    - Network Elements can be added.
    - Advanced Configuration settings that were valid for 12.5.0/12.5.0.4/12.6.0 may be changed.

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP from 12.5.0/12.5.0.4 to Release 12.6. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to Release 12.6.1.

Policy Management Components	CMP Release 12.6.1	MRA Release 12.6.1	MPE Release 12.6.1
MRA release 12.5.0/12.5.0.4/12.6.0	Yes	Yes	Yes
MPE release 12.5.0/12.5.0.4/12.6.0	Yes	Yes	N/A

2.3.3 Supported Software Releases Rollback (Backout) Support and Limitation

- After the entire Policy Management system is upgraded to Release 12.6.1, you may decide that a backout to the previous release is required. In that case, each individual server/cluster must be backed out.
- If it is necessary to backout multiple servers, it is required that the systems be rolled back in the reverse order in which they were upgraded. This implies that all the related component servers are rolled back first before the active CMP/NW-CMP and DR-CMP/NW-CMP can be rolled back to the previous version.
- After all the servers in the system are backed out to the previous release, the servers could be upgraded to another supported minor or major release for example, if all of the servers in the Policy Management system were backed out from Release 12.6.1 to 12.5.0/12.5.0.4/12.6.0, these servers could subsequently be upgraded to Release 12.6-Build_A.

- Backout may be performed at any time after the upgrade, with these general limitations:
  - If a new features has been enabled, it must be disabled prior to any backout.
  - If there is an unexpected problem that requires backout after a feature has been enabled, it is possible that transient subscriber data, which is changed by the new feature, may be impacted by the unexpected problem. In this situation, those sessions cannot be guaranteed to be unaffected for any subsequent actions (this includes any activity after the feature is disabled). This may prevent data restoration by the SSDP feature during the backout. The impact of any unexpected problem must be analyzed when it occurs to determine the best path forward (or backward).

    NOTE: Although backout after feature activation is allowed, due to the number of possible permutations under which new features may be activated, the only testing that is performed is based on backout without new feature activation.
  - Backout can only be used to go back one release. This restriction applies to all types of releases including any major, minor, maintenance, or incremental release including minor releases of Release 12.6.

2.3.3.1 Rollback (Backout) Sequence

The Rollback of Policy Management system from Release N+1 to Release N is generally performed in this order (reverse of the Upgrade sequence):

NOTE: See the related upgrade/rollback upgrade paths for more detail procedures. These procedures are not documented in this document.

Release 12.6.1 to Release 12.5.0/12.5.0.4/12.6.0 (Wireless mode only)

1. MRA clusters, including spare server if geo-redundancy is deployed.
2. MPE clusters, including spare server if geo-redundancy is deployed.
3. Standalone Primary CMP/S-CMP and Disaster Recovery (DR) CMP/S-CMP clusters.
4. If multi-level OAM is deployed, Primary NW-CMP primary cluster and Disaster Recovery (DR) NW-CMP cluster.

2.4 Migration of Policies and Supporting Policy Data

The existing Policies configuration and Subscriber Session information is conserved during the upgrade.

3. CHANGES BY FEATURE

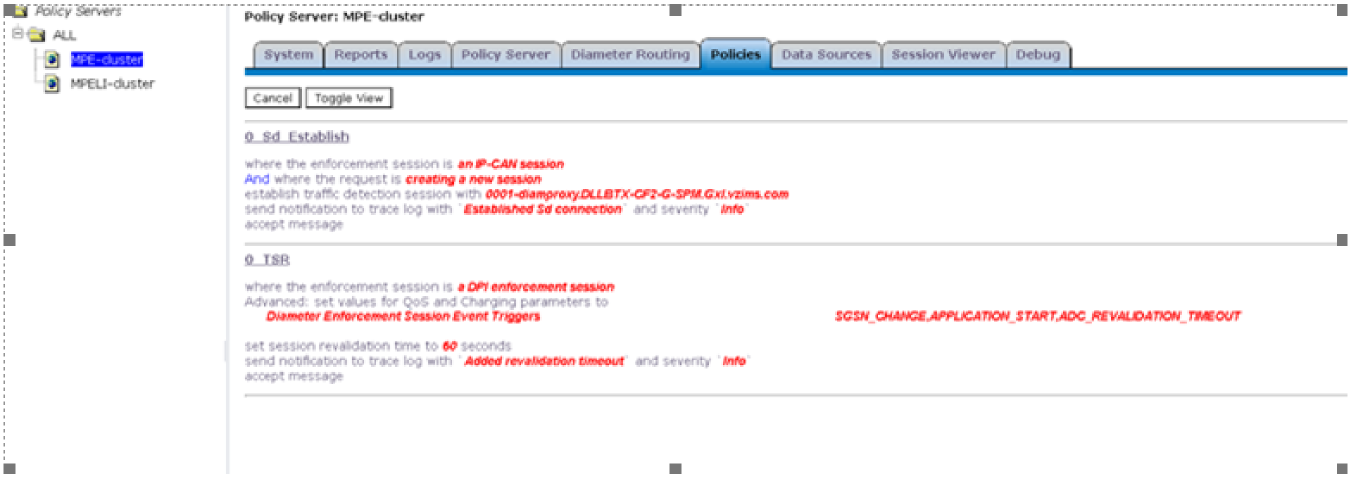
3.1 Revalidation-Timeout event trigger over Sd Interface (Bug 32817743)

3.1.1 Introduction

With this enhancement, Sd interface now supports both the **ADC_REVALIDATION_TIMEOUT** and **REVALIDATION_TIMEOUT** event triggers and **Revalidation-time (1042)** and **DC_Revalidation_Time (2801)** AVPs in the TSR message to revalidate a TDFsession on the Sd interface**.**

3.1.2 Sample Policy

Configure the policy as below:



0_Sd_Establish

where the enforcement session is *an IP-CAN session*
And where the request is *creating a new session*
establish traffic detection session with *0001-diamproxy.DLLBTX-CF2-G-SPM.Gxl.vzims.com*
send notification to trace log with `*Established Sd connection*` and severity `*Info*`
accept message

0_TSR

where the enforcement session is *a DPI enforcement session*
Advanced: set values for QoS and Charging parameters to
Diameter Enforcement Session Event Triggers *SGSN_CHANGE,APPLICATION_START,ADC_REVALIDATION_TIMEOUT*

set session revalidation time to *60* seconds
send notification to trace log with `*Added revalidation timeout*` and severity `*Info*`
accept message

3.1.3 Detailed Description:-

NOTE: - Default event triggers will appear in diameter message when there is no event trigger configured in the policy. (As per before fix)

The event trigger in the Sd interface works based the configuration of event trigger in the above policy action.

1. If we have configured ADC_REVALIDATION_TIMEOUT in the policy, then the output of TSR message contains ADC_REVALIDATION_TIMEOUT event trigger along with ADC_Revalidation_Time (2801) AVP.
2. If we have configured REVALIDATION_TIMEOUT in the policy, then the output of TSR message contains REVALIDATION_TIMEOUT event trigger along with Revalidation_Time (1042) AVP.
3. If we have configured both ADC_REVALIDATION_TIMEOUT, REVALIDATION_TIMEOUT in the policy, then the output of TSR message contains REVALIDATION_TIMEOUT , ADC_REVALIDATION_TIMEOUT event trigger along with Revalidation_Time (1042) AVP, ADC_Revalidation_Time (2801).
4. If we set the revalidation time in the policy it won't add default REVALIDATION_TIMEOUT trigger in the output of TSR message.
5. If we set the revalidation time in the policy along with the configured event trigger depending on ADC_REVALIDATION_TIMEOUT or REVALIDATION_TIMEOUT, then in the output of TSR message contains respective event trigger.

4. PROTOCOL FLOW/PORT CHANGE

No Changes

5. MEAL INSERTS

There are no changes to Alarms, Measurements, KPIs and MIBs.