Hardware and Software

ORACLE

Engineered to Work Together

Oracle® Communications

Policy Management
Network Impact Report

Release 12.3

E85330-01

July 2017

Oracle Communication Policy Management Network Impact Report
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Figures

Tables

1. INTRODUCTION

1.1 Purpose and Scope

This document highlights the changes in Oracle Communication Policy Management Release 12.3 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 12.3 new and enhancement features as compared to previous release of 12.1.x/12.2.x and the operations impacts of these features, at a high level. The Feature Requirements (FRS) documents remain the defining source for the expected behavior of these features.

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.

Acronym	Definitions
GUI	Graphical User Interface
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

Acronym	Definitions
PCEF	Policy and Charging Enforcement Function (GGSN, PGW, DPI)
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 12.3 FEATURES

This section provides an overview list of the Policy Management Release 12.3 new features.

1.1 Policy Management release 12.3 New Features Support

Feature Number	Feature Name
22135911	7.124 // 7.918 (3GPP: Rule-Activation support for QoS Information in Gx.)
23081328	Policy Configuration Management over OSSI Interface
23634069	Add support for VMWare in NF Agent
20396273	VNF Orchestration/NSO
24522459	Password expiration time must be implemented (60 days)
24522481	Permits in the files with sensible information must be implemented so these are only property of root.
24522484	Security certificate of the SSL/TLS current and valid must be used.
24750030	Time Conditional ARP and QCI
25241720	MRA Associations Backup and Restore
23173988	Policy Management Virtualized Software Bundle
22315343	Revalidation Timer Randomization Feature
24953778	NB-IoT - Cat M2 device support
25173137	MySQL root password is modifiable

2.1 Policy Management Hardware Requirements

2.1.1 Supported Hardware

The Policy Management Release 12.3 software can be deployed on the hardware that was previously supported under Release 12.1.x/12.2.x:

- Oracle NETRA Server X5-2.
- Oracle Server X5-2 on Rack Mount Server (RMS).
- 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 server is NOT supported

2.2 Policy Management Software Changes

2.2.1 Software Components

Components	Releases
TPD 64 Bit	7.0.3
COMCOL	6.4
PM&C	6.0.3
TVoE	3.0.3
AppWorks	6.0.1
Networking	6.0.3
HP Firmware FUP	2.2.9 (Minimum) 2.2.10 (Current)
Oracle Firmware	3.1.5 (Minimum) 3.1.6 (Current)

2.2.2 UDR and SPR Product Compatibility

Products	Releases	Compatibility
Oracle Communication UDR*	12.2	MPE via Sh interface and CMP via RESTful API. Use of Profile V2, Profile V3, and Profile V4 schemas.

***NOTE:** Policy R12.3 does not support Oracle SDM SPR Release 9.3.1

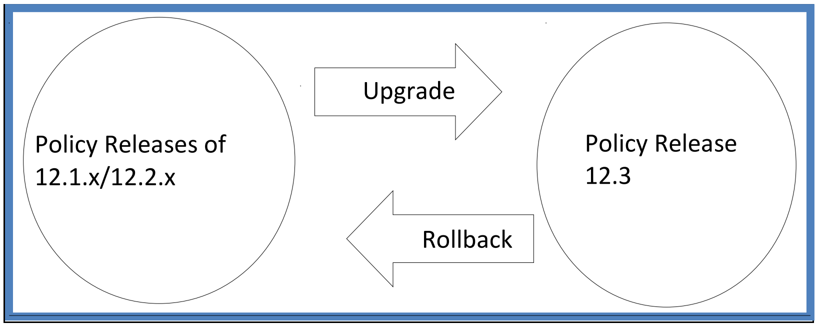
2.3 Policy Management Software Upgrade/Backout Overview

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 12.3

Figure 1shows the supported upgrade Path for Release 12.3

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 12.1.x or 12.2.x prior to upgrading to this release (12.3). This applies to wireless and fixed line.

2.3.2 Mixed Version Policy Management System Expectations

The system that is running Release 12.1.x/12.2.x mixed configuration supports the performance and capacity of Release 12.1.x/12.2.x respectively. The mixed version Policy Management configuration supports Release 12.1.x/12.2.x features respectively.

In the mixed version Policy Management configuration, Release 12.3 CMP has these general limitations:

- New features must not be enabled until the upgrades of all servers managed by that CMP are completed. This also applies to using policy rules that include new conditions and actions introduced in the release.
- 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 12.1.x/12.2.x may be changed.

NOTE: Replication between CMP and DR-CMP is automatically disabled during upgrade of CMP and DR-CMP from Release 12.1.x/12.2.x to Release 12.3. The replication is automatically enabled after both active CMP and DR-CMP are upgraded to Release 12.3.

Policy Management Components	**CMP Release 12.3**	**MRA Release 12.3**	**MPE Release 12.3**
CMP release 12.1.x/12.2.x	No	No	No
MRA release 12.1.x/12.2.x	Yes	Yes	Yes
MPE release 12.1.x/12.2.x	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 12.3, 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 12.3 to Release 12.1.x/12.2.x, these servers could subsequently be upgraded to Release 12.3-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 12.3.

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. See the Policy Management Release 12.3 documentation.

Release 12.3 to Release 12.1.x/12.2.x (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

1.1 7.124 // 7.918 (3GPP: Rule-Activation support for QoS Information in Gx.) (PR 22135911)

3.1.1 Pre-Requisite

This feature reduces the network congestion which results from a large number of simultaneous APN-AMBR Default-EPS-Bearer-QoS value changes.

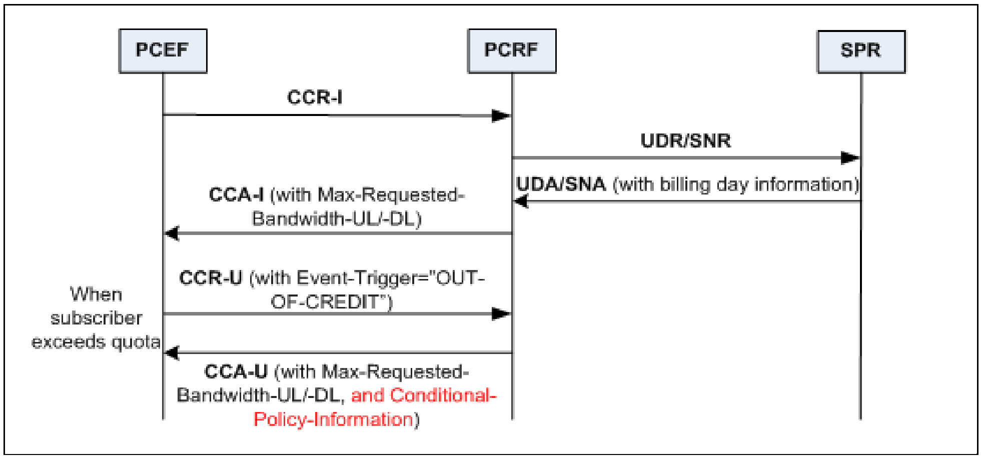
3.1.2 Introduction

This feature enhancement implements time based rule-activation for QoS Information in Gx interface through CCA and RAR procedures. This enhancement also enables you to randomize the time at which the PCEF updates APN-AMBR and DEBQ values and then sends it on Gx or Gx-lite interface through Conditional Policy Information AVP.

3.1.3 Detailed Description

Policy Management can specify when APN-AMBR/DEBQ values should be reset to their non-throttled values in the same message which initiates the throttling. Figure 9 shows the call flow that explains using Condition-Policy-Information AVP.

Figure 2 Call Flow Using Condition-Policy-Information AVP


PCEF
PCRF
SPR
CCR-I
UDR/SNR
UDA/SNA (with billing day information)
CCA-I (with Max-Requested-Bandwidth-UL/-DL)
CCR-U (with Event-Trigger="OUT-OF-CREDIT")
When subscriber exceeds quota
CCA-U (with Max-Requested-Bandwidth-UL/-DL, and Conditional-Policy-Information)

This implementation has its limit, that is if there is a DRA or any Diameter Peer device between the MRA and PCEF (PGW), then the MRA is interpreted as the direct Diameter connection to the PCEF is down, thus no SDR message is sent out.

3.1.4 Policy Changes

This section describes the new policy actions (optional policy actions) added/modified as part of this enhancment.

Table 2 New Policy Actions

Policy Condition Group	Policy Condition or Action	Description
Setting a state variable policy action.	set the **scope** state variable **name** to **time** **plus** random value within **#** seconds and save **always**.	Set a state variable with specified scope and name to a time with/without randomization added to it. *scope*: specifies scope of the variable we are creating in this policy action. *name*: specifies name of the variable we are creating in this policy action. *time*: here we configure the time in different ways - Specific time - Relative time - Policy counter id - Day Of Week You can also configure a state variable here which holds time, by selecting the **Specific time** option. *plus*: Supports the these values: - plus - minus - plus/minus #: Specifies random value range. a*lways*: Select from these options: - always (default) - unless rejected

Policy Condition Group	Policy Condition or Action	Description
Setting Conditional Policy Information AVP Action	overwrite Conditional Policy Information with Execution-Time to time and parameters specified.	Set Conditional-Policy-Information AVP with specified values. *overwrite*: Use to configure whether Conditional-Policy-Information AVP must be added/appended to existing list or removed existing ones and added new one. - overwrite - add *time*: Use to configure the time in different ways. - Specific time - Relative time - Policy counter id - Day Of Week You can also configure a state variable here which holds time, by selecting the **Specific time** option. *specified*: This field allows you to configure APN-AMBR-UL/DL values and DEBQ (QCI and ARP) values.

Table 3 Modified Policy Actions

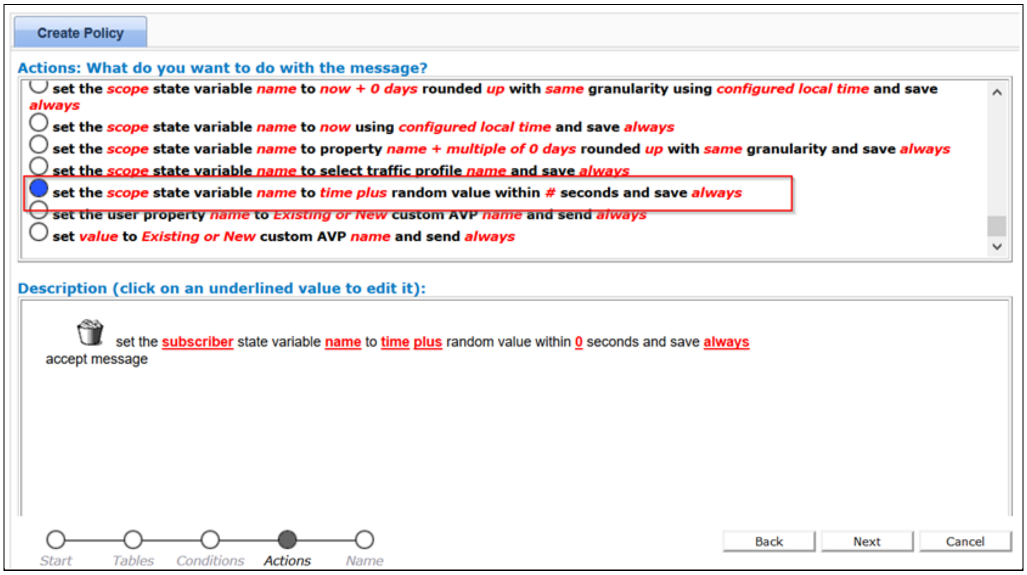
Policy Condition Group	Policy Condition or Action	Description
Install PCC rules with activation and deactivation time.	install specified PCC rule(s) for select scope active between start time and end time.	Installs PCC rules for selected scope and with activation and deactivation time. As part of this feature we are modifying this field: *start time and end time*: This field can be configured using a drop down which allows you to select from specific time, relative time and Policy Counter ID. Currently (before this feature) Specific Time does not support Policy variable substitution. As part of this feature, specific time supports Policy variable substitution. Other fields are unchanged.

Policy Condition Group	Policy Condition or Action	Description
Install PCC rules with activation and deactivation time with a retry profile.	`install specified PCC rule(s) for select scope for specified retry profile active between start time and end time`	Installs PCC rules for selected scope and with activation and deactivation time. As part of this feature we are modifying this field *start time and end time*: This field can be configured using a drop down which allows you to select specific time, relative time, or Policy Counter ID. Currently (before this feature) Specific Time does not support Policy variable substitution. As part of this feature, specific time supports Policy variable substitution. Other fields are unchanged.

3.1.5 User Interface Changes

The two new policy actions used to set Conditional-Policy-Information AVP

CMP GUI: Navigate to **POLICY MANAGEMENT → Policy Library → Create Policy**



Actions: What do you want to do with the message?

○ set the *scope* state variable *name* to *now + 0 days* rounded *up* with *same* granularity using *configured local time* and save *always*

○ set the *scope* state variable *name* to *now* using *configured local time* and save *always*

○ set the *scope* state variable *name* to property *name + multiple of 0 days* rounded *up* with *same* granularity and save *always*

○ set the *scope* state variable *name* to select traffic profile *name* and save *always*

● set the *scope* state variable *name* to *time plus* random value within *#* seconds and save *always*

○ set the user property *name* to *Existing or New* custom AVP *name* and send *always*

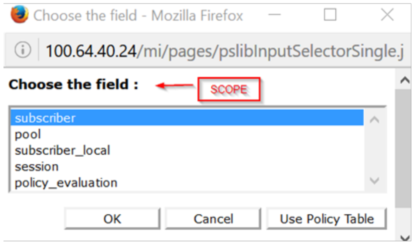
○ set *value* to *Existing or New* custom AVP *name* and send *always*

Description (click on an underlined value to edit it):

set the subscriber state variable name to time plus random value within 0 seconds and save always

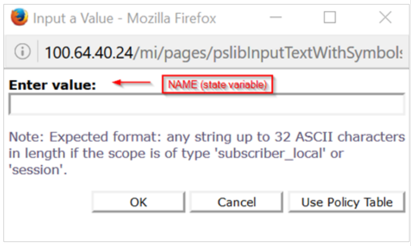
accept message

The GUI screens to configure the fields in the selected policy actions are:


Choose the field - Mozilla Firefox
100.64.40.24/mi/pages/pslibInputSelectorSingle.j
SCOPE
OK
Cancel
Use Policy Table

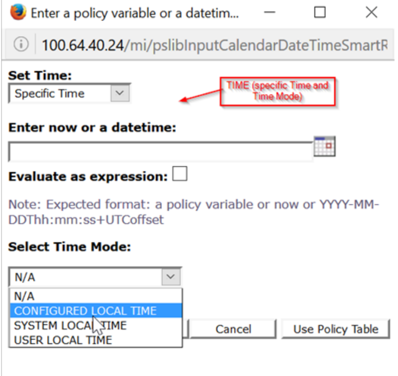
Choose the field :

- subscriber
- pool
- subscriber_local
- session
- policy_evaluation


Input a Value - Mozilla Firefox
100.64.40.24/mi/pages/pslibInputTextWithSymbol
NAME (state variable)
OK
Cancel
Use Policy Table

Enter value:

Note: Expected format: any string up to 32 ASCII characters in length if the scope is of type 'subscriber_local' or 'session'.


Enter a policy variable or a datetim...
100.64.40.24/mi/pages/pslibInputCalendarDateTimeSmartR
TIME (specific Time and Time Mode)
Cancel
Use Policy Table

Set Time: Specific Time

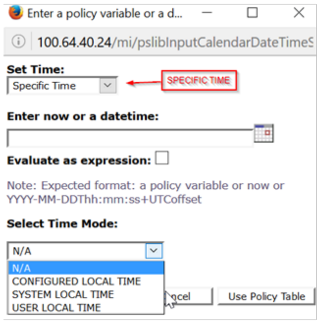
Enter now or a datetime:

Evaluate as expression: □

Note: Expected format: a policy variable or now or YYYY-MM-DDThh:mm:ss+UTCoffset

Select Time Mode: N/A

- N/A
- CONFIGURED LOCAL TIME
- SYSTEM LOCAL TIME
- USER LOCAL TIME


Enter a policy variable or a d...
100.64.40.24/mi/pslibInputCalendarDateTimeS
SPECIFIC TIME
Cancel
Use Policy Table

Set Time: Specific Time

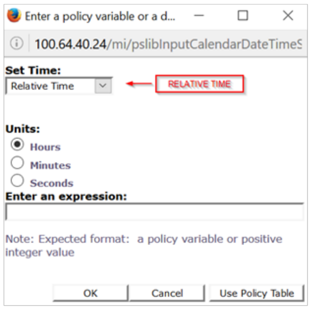
Enter now or a datetime:

Evaluate as expression: □

Note: Expected format: a policy variable or now or YYYY-MM-DDThh:mm:ss+UTCoffset

Select Time Mode: N/A

- N/A
- CONFIGURED LOCAL TIME
- SYSTEM LOCAL TIME
- USER LOCAL TIME


Enter a policy variable or a d...
100.64.40.24/mi/pslibInputCalendarDateTimeS
RELATIVE TIME
OK
Cancel
Use Policy Table

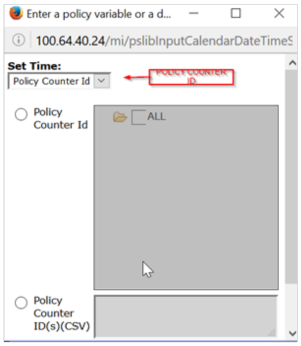
Set Time: Relative Time

Units:

● Hours
○ Minutes
○ Seconds

Enter an expression:

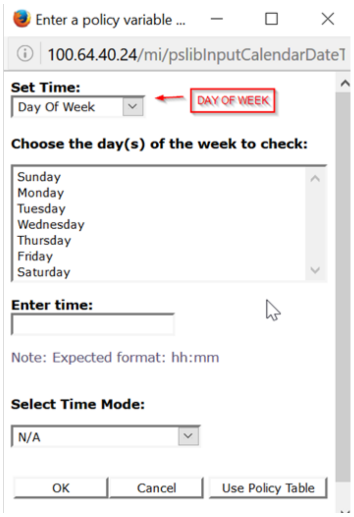
Note: Expected format: a policy variable or positive integer value


Enter a policy variable or a d...
100.64.40.24/mi/pslibInputCalendarDateTimeS
POLICY COUNTER ID
ALL

Set Time: Policy Counter Id

○ Policy Counter Id

○ Policy Counter ID(s)(CSV)


Enter a policy variable ...
100.64.40.24/mi/pslibInputCalendarDateT
DAY OF WEEK
OK
Cancel
Use Policy Table

Set Time: Day Of Week

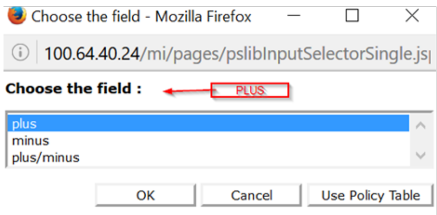
Choose the day(s) of the week to check:

- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

Enter time:

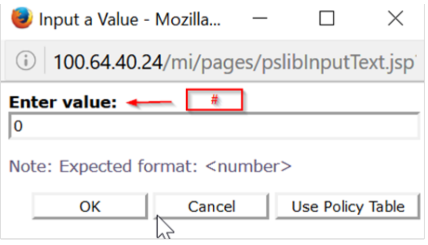
Note: Expected format: hh:mm

Select Time Mode: N/A


Choose the field - Mozilla Firefox
100.64.40.24/mi/pages/pslibInputSelectorSingle.js
PLUS
OK
Cancel
Use Policy Table

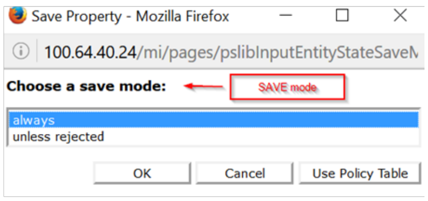
Choose the field :

- plus
- minus
- plus/minus


Input a Value - Mozilla...
100.64.40.24/mi/pages/pslibInputText.jsp
#
OK
Cancel
Use Policy Table

Enter value: 0

Note: Expected format: <number>


Save Property - Mozilla Firefox
100.64.40.24/mi/pages/pslibInputEntityStateSaveM
SAVE mode
OK
Cancel
Use Policy Table

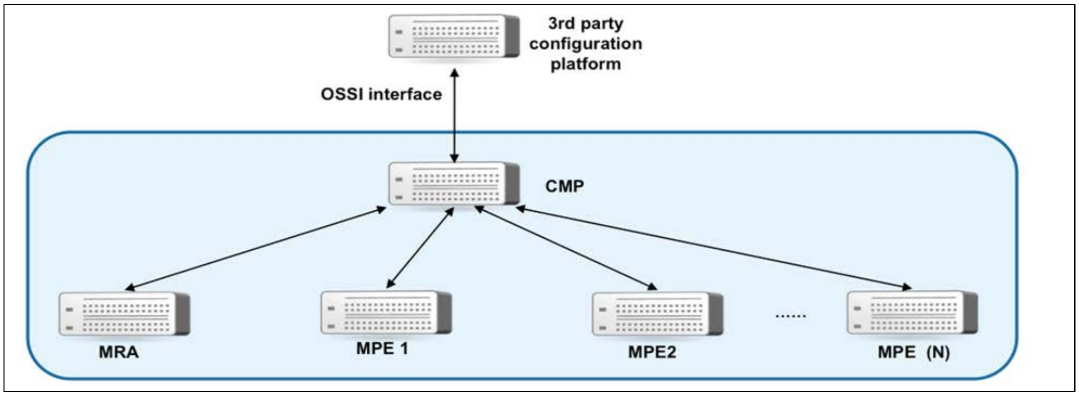
Choose a save mode:

- always
- unless rejected

3.2 Policy Configuration Management over OSSI Interface (PR 23081328)

3.2.1 Introduction

The Policy Management OSSI/XML interface is designed for transferring the Policy scripts from a third party system to MPE server, and executing the import missions. When the Policy Scripts are transferred from the third party system to CMP using the OSSI/XML interface and deployed to MPE server, the script execution results (and error messages) are also transferred from the CMP to the third party system using OSSI/XML interface.



This feature enhances the existing supported OSSI XML interfaces such as Common, Topology, Subscriber, and Operational Measurements, by adding the these Policy XML operation interfaces:

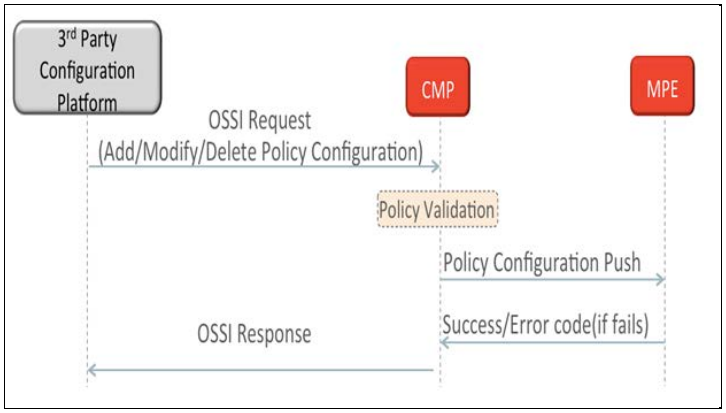
- Add new policy configuration
- Modify the existing policy configuration
- Delete existing policy configuration
- Policy configuration Import and Export

3.2.2 Detailed Description

Figure 2 shows the general call flow for:

- Adding new policy configuration
- Modifying/Deleting the existing policy configuration

Figure 3 General Call Flow with OSSI

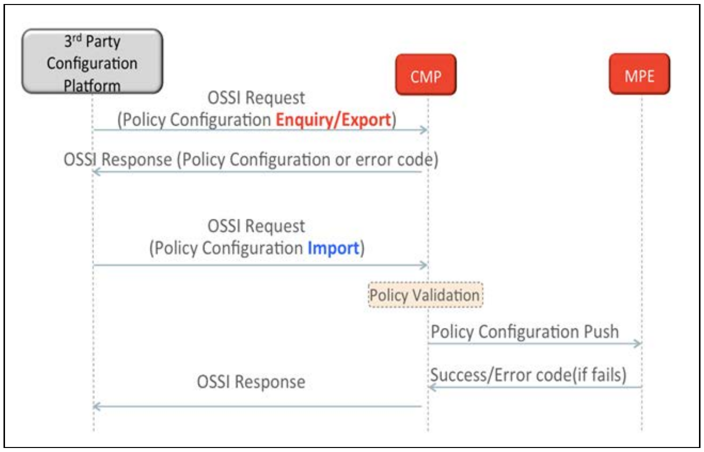

3rd Party Configuration Platform
CMP
MPE
OSSI Request (Add/Modify/Delete Policy Configuration)
Policy Validation
Policy Configuration Push
Success/Error code(if fails)
OSSI Response

1. Third party configuration platform send the OSSI request with the policy configuration actions as (Add new policy configuration, Modify/Delete the existing policy configuration)

2. With the OSSI request received, CMP validates the policy configuration in the OSSI request and feedback the error to third party configuration platform if there is
3. If there is not any errors in the policy configuration in OSSI messages, CMP pushes the policy configuration to the corresponding MPE servers
4. MPE servers feed back the results of policy configuration (Success/Error Code if it fails)
5. CMP feeds back the OSSI request result to the configuration platform
6. CMP generates the system logs for the operations

Figure 3 shows the general call flow for the import and export of existing policy configuration

Figure 4 General Call Flow for OSSI Import and Export


3rd Party Configuration Platform
CMP
MPE
OSSI Request (Policy Configuration Enquiry/Export)
OSSI Response (Policy Configuration or error code)
OSSI Request (Policy Configuration Import)
Policy Validation
Policy Configuration Push
Success/Error code(if fails)
OSSI Response

3.2.2.1 Policy Configuration Export

1. Third party configuration platform send the OSSI request with the request of policy configuration export/enquiry
2. CMP feeds back the exported policy configuration or error code (if the operation fails) in OSSI response message

3.2.2.2 Policy Configuration Import

1. Third party configuration platform send the OSSI request with the request of policy configuration import
2. With the OSSI request received, CMP validates the policy configuration in the OSSI request and feeds back the error to third party configuration platform if there is one.
3. If there is not any errors in the policy configuration OSSI messages that the third party platform is expected to import, the CMP pushes the policy configuration to the corresponding MPE servers
4. MPE servers feedback the result of policy configuration (Success or Error Code if it fails)
5. The CMP feeds back the OSSI request result to the configuration platform

This code shows the general format for Policy XML operation interface:

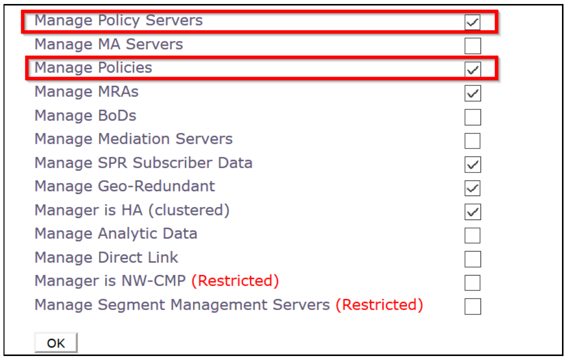
```
<XmlInterfaceRequest>
  < (Policy XML Operation tag name) >
    <Policy>
        <Name> (policy name) </Name>
        <Description> (policy description detail) </Description>
        <ActionValues> ….. </ActionValues>
        <ConditionValues> ….. </ConditionValues>
        <ConditionVariables> ….. </ConditionVariables>
        <Analytics> (False/True) </Analytics>
     </Policy>
<PolicyGroup>
        <Name> (policy group name) </Name>
        <Description> (policy group description detail) </Description>
        <RootGroup> (False/True) </RootGroup>
        <ElementRef>
            <Name> (policy name) </Name>
            <SubGroup> (False/True) </SubGroup>
        </ElementRef>
  </PolicyGroup>
</(Policy XML Operation tag name) >
</XmlInterfaceRequest>
```

3.2.3 User Interface Changes

Figure 5 shows the CMP mode options to enabled for this feature:

- Manage Policy Servers
- Manage Policies

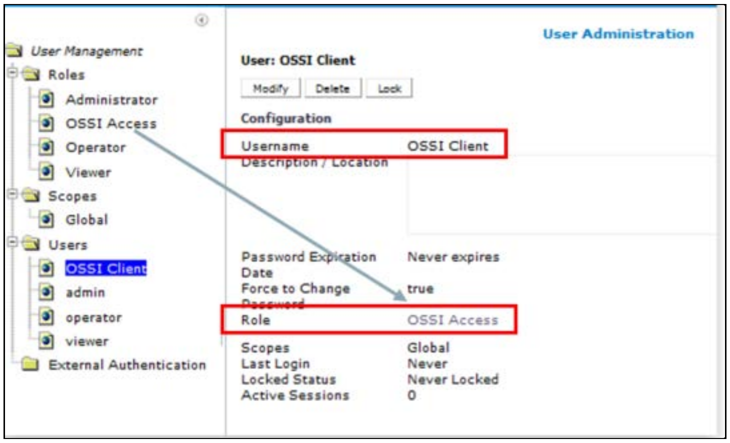
Figure 5 CMP Modes to Enable OSSI Policy Support



Manage Policy Servers ☑
Manage MA Servers ☐
Manage Policies ☑
Manage MRAs ☑
Manage BoDs ☐
Manage Mediation Servers ☐
Manage SPR Subscriber Data ☑
Manage Geo-Redundant ☑
Manager is HA (clustered) ☑
Manage Analytic Data ☐
Manage Direct Link ☐
Manager is NW-CMP (Restricted) ☐
Manage Segment Management Servers (Restricted) ☐

Additional CMP user access account could be created for the third-party OSSI client associated with the required role.

CMP GUI: Navigate to **System Administration → User Management → Users → <*login name*>** where the <*login name*> is OSSI Client with OSSI Access role as an example.



User: OSSI Client

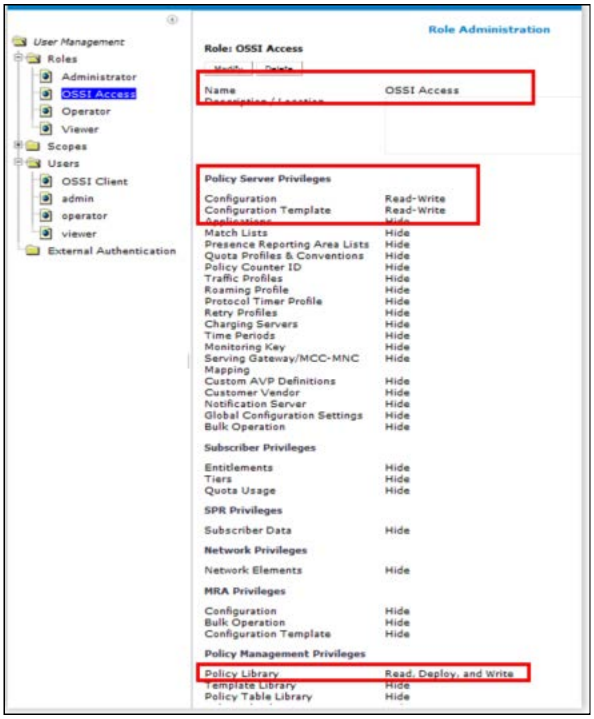
Configuration

Username	OSSI Client
Description / Location	
Password Expiration Date	Never expires
Force to Change Password	true
Role	OSSI Access
Scopes	Global
Last Login	Never
Locked Status	Never Locked
Active Sessions	0

The third-party OSSI client should have these CMP related access privileges*(role) to perform the Policy XML Operation:

- Policy Library set to Read, Deploy and Write
- Policy Server Configuration set to Read-Write
- Policy Server Configuration Template set to Read-Write

CMP GUI: Navigate to **System Administration → User Management → Roles → <***Role name***>**



Role: OSSI Access

Name	OSSI Access
Description / Location	
Policy Server Privileges	
Configuration	Read-Write
Configuration Template	Read-Write
Applications	Hide
Match Lists	Hide
Presence Reporting Area Lists	Hide
Quota Profiles & Conventions	Hide
Policy Counter ID	Hide
Traffic Profiles	Hide
Roaming Profile	Hide
Protocol Timer Profile	Hide
Retry Profiles	Hide
Charging Servers	Hide
Time Periods	Hide
Monitoring Key	Hide
Serving Gateway/MCC-MNC Mapping	Hide
Custom AVP Definitions	Hide
Customer Vendor	Hide
Notification Server	Hide
Global Configuration Settings	Hide
Bulk Operation	Hide
Subscriber Privileges	
Entitlements	Hide
Tiers	Hide
Quota Usage	Hide
SPR Privileges	
Subscriber Data	Hide
Network Privileges	
Network Elements	Hide
MRA Privileges	
Configuration	Hide
Bulk Operation	Hide
Configuration Template	Hide
Policy Management Privileges	
Policy Library	Read, Deploy, and Write
Template Library	Hide
Policy Table Library	Hide

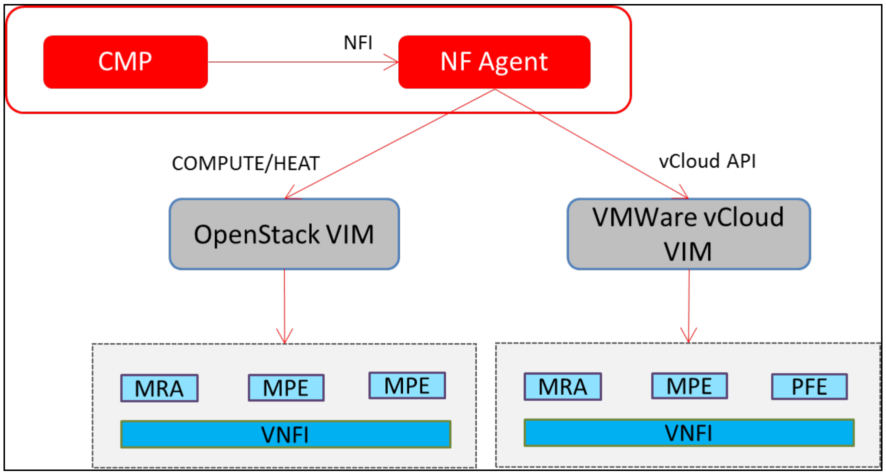
3.3 Add support for VMWare in NF Agent (PR 23634069)

3.3.1 Introduction

Release 12.2 introduced the NF Agent with support for OpenStack. As part of the continuing effort to improve support for cloud deployments, release 12.3 introduces support for VMware vCloud Director within NF Agent.

3.3.2 Detailed Description

The NF Agent interacts with VIMs to request the creation or termination of cluster VMs. In 12.2, the only type of VIM supported was OpenStack. In 12.3, NF Agent adds support for VMware vCloud VIMs:

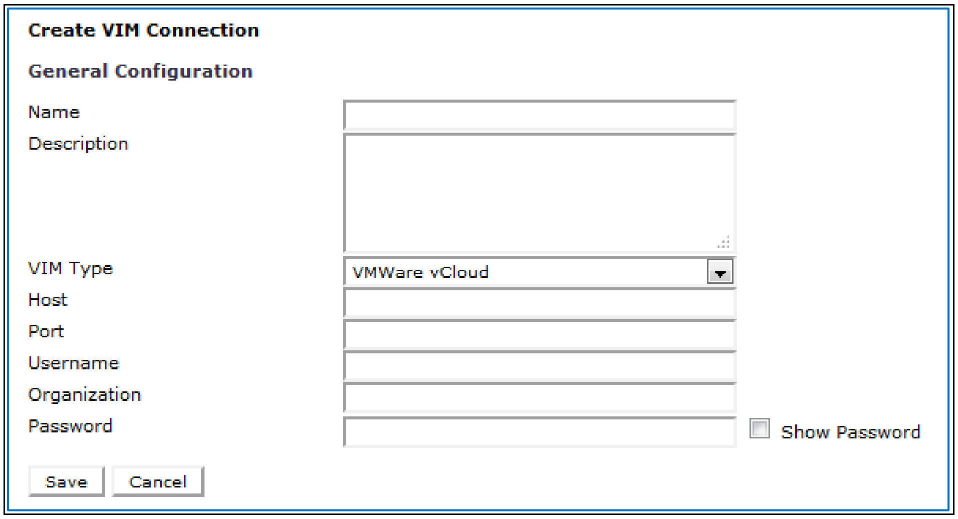


3.3.3 User Interface Changes

3.3.3.1 VIM Type

In the CMP GUI, under **NF MANAGEMENT → VIM Connections** a new VIM type has been added when creating a VIM. The type is **VMWare vCloud**.

Figure 6 Create VIM Connection



Create VIM Connection

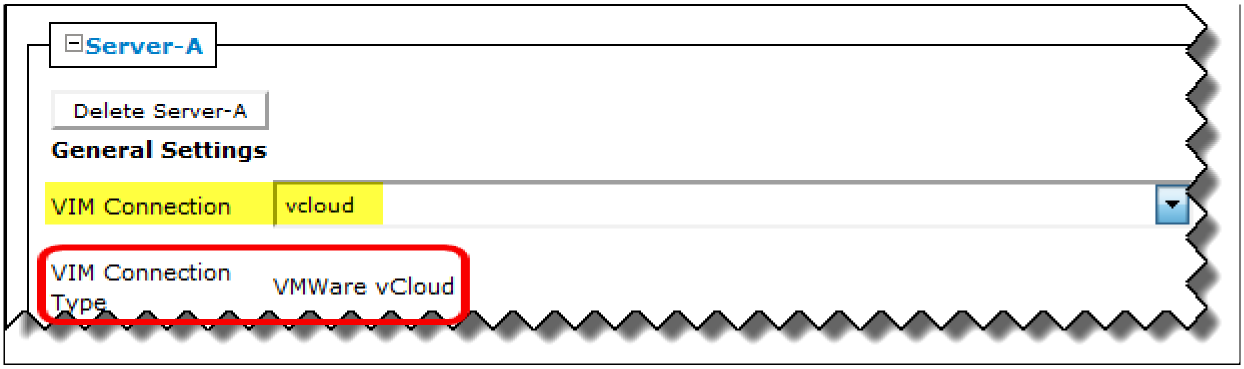
General Configuration

Name	
Description	
VIM Type	VMWare vCloud
Host	
Port	
Username	
Organization	
Password	

Selecting the **VMware vCloud** VIM type displays the appropriate set of configuration fields as shown in Figure 1.

3.3.3.2 *New MPE/MRA Cluster*

When creating a new MPE/MRA cluster, the VIM Connection Type appears as VMware vCloud when the selected VIM Connection is of this type.



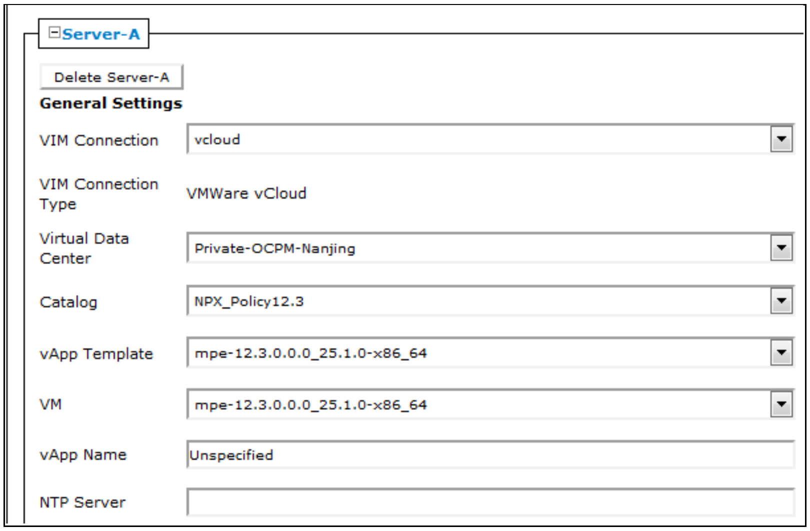
General Settings

VIM Connection: vcloud

VIM Connection Type: VMWare vCloud

A number of additional fields appear when the VIM Connection is of type VMware vCloud.

- The VDC (Virtual Data Center) where the resources are located
- The Catalog where the vApp Templates reside in
- The vApp Template to use
- The VM to be created
- The name to be given to the vApp instance (if it doesn't exist)



General Settings

VIM Connection: vcloud

VIM Connection Type: VMWare vCloud

Virtual Data Center: Private-OCPM-Nanjing

Catalog: NPX_Policy12.3

vApp Template: mpe-12.3.0.0.0_25.1.0-x86_64

VM: mpe-12.3.0.0.0_25.1.0-x86_64

vApp Name: Unspecified

NTP Server:

This information is based on the topology and provided by the local vCloud Director administrator.

3.3.3.3 *Alarms and Logs*

No new measurements, alarms, or logs are introduced with this feature. The same alarms and logs used in 12.2 apply.

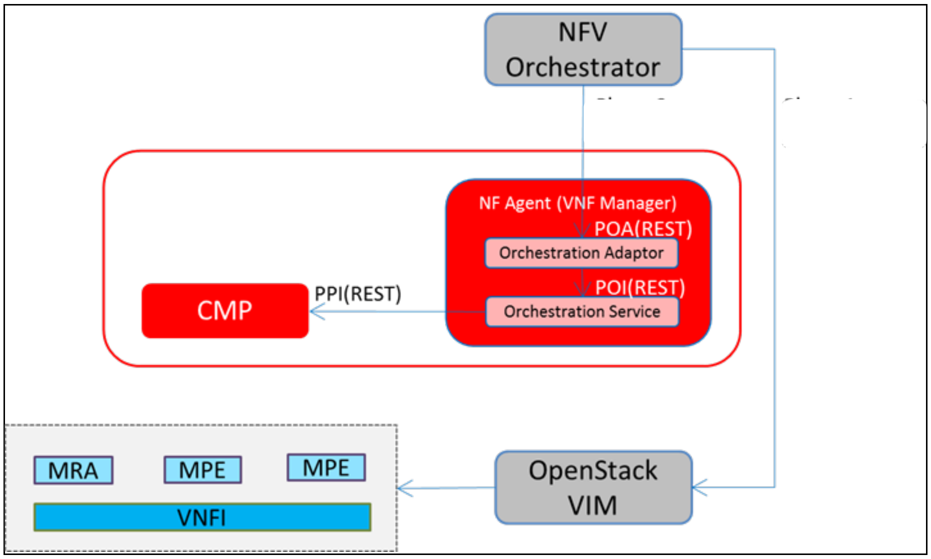
3.4 VNF Orchestration/NSO (PR 20396273)

3.4.1 Introduction

Oracle customers expect greater degree of life-cycle automation. Policy Management 12.3 introduces capabilities to allow orchestration as per the NFV-MANO architecture model.

3.4.2 Detailed Description

Policy orchestration use cases are supported with the implementation of two layers in the NF Agent:



The NF Agent Orchestration Adaptor acts as a front-end to the NF Agent:

- It hides differentiation among orchestration standards
- It can adapt to different orchestration protocols
- It translates messages to the internal Orchestration Service

The NF Agent Orchestration Service carries out the internal orchestration functions. For example, it applies service configuration to a VNF managed by CMP

NF Agent orchestration includes support for VNF deployment and scaling where resource allocation is performed by an orchestrator using Heat templates.

3.4.3 User Interface Changes

3.4.3.1 Sample Templates

A Policy 12.3 system comes preloaded with a set of sample templates to support deployment and scaling in/out. These sample templates can be customized to fit your topology.

The sample templates correspond to these levels:

Level 0: Deployment of CMP and NF Agent

Level 1: Scale out an MRA and an MPE

Level 2: Scale out an MPE and associate it with an existing MRA

Level 3: Scale out an MRA and two associated MPEs

The sample Heat templates can be found in the CMP server under `/etc/camiant/vnf/templates/nso/`:

```
pcrf_level0.heat.yaml

pcrf_level1.heat.yaml

pcrf_level2.heat.yaml

pcrf_level3.heat.yaml
```

A simplified sample Heat template level 0 looks like this:

```
parameters:
  ntp:
    type: string
    default: 10.210.60.196
  mode:
    type: string
    default: Wireless
  mimode:
    type: string
    default:'SMPP,DiamAF,Diam3gppPCEF'
  oam_network: …
  siga_network: …
  sigb_network: …
  sigc_network: …
  cmp_image: …
  mra_image: …
  mpe_image: …
  flavor: …
  availability_zone: …
resources:
  CMPSITE1_OAM:
    properties: {network:
      {get_param: oam_network},
      port_security_enabled: false}
    type: OS::Neutron::Port
  CMPSITE1_SERVERA: …
  CMPSITE1_SERVERA_OAM: …
  CMPSITE1_SERVERA_SIGA: …
  CMPSITE1_SERVERA_SIGB: …
  CMPSITE1_SERVERA_SIGC: …
  CMPSITE1_SERVERB: …
  CMPSITE1_SERVERB_OAM: …
  CMPSITE1_SERVERB_SIGA: …
  CMPSITE1_SERVERB_SIGB: …
  CMPSITE1_SERVERB_SIGC: …
outputs:
  LEVEL:
     value: 0
  CMPSITE1_OAM_IP:
     value: {get_attr: [CMPSITE1_OAM,
           fixed_ips, 0, ip_address]}
  CMPSITE1_SERVERA_OAM_IP: …
  CMPSITE1_SERVERB_OAM_IP: …
  CMPSITE1_OAM_CIDR: …
  CMPSITE1_SERVERA_OAM_CIDR: …
  CMPSITE1_SERVERB_OAM_CIDR: …
```

3.4.3.2 Service Configuration Files

In addition to Heat templates, the NF Agent orchestration layers also use Service Configuration files to receive additional topology and configuration information.

The sample service configuration files are located in `/opt/camiant/vnfmgr/cfg/poi/`

```
OCPM_Topology_ServiceConfig_1.json
OCPM_Topology_ServiceConfig_2.json
OCPM_Topology_ServiceConfig_3.json
```

Notice there are three service configuration files (1 through 3) versus four Heat templates (1 through 4). Heat template level 0 is for CMP/NF Agent deployment and the configuration is done manually not using a file.

A sample service configuration file for level 2 looks like this:

```
{
  "mras":[{"mraSystemConfig":{"name":"MRA1-1"},
           "mraConfig":{"diameterIdentity":"mra11",
                        "diameterRealm":"oracle.com"},
            "associatedTemplates":["mraTemplate"],
            "associatedMpes":[{"mpeName":"MPE1-1-1"},
                            {"mpeName":"MPE1-1-2"}]}],
  "mpes":[{"clusterName":"MPE1-1-1",
           "mpeSystemConfig":{"name":"MPE1-1-1"},
            "mpeConfig":{"diameterIdentity":"mpe111",
                        "diameterRealm":"oracle.com"},
            "associatedTemplates":["mpeTemplate"]},

         {"clusterName":"MPE1-1-2",
           "mpeSystemConfig":{"name":"MPE1-1-2"},
           "mpeConfig":{"diameterIdentity":"mpe112",
                        "diameterRealm":"oracle.com"},
           "associatedTemplates":["mpeTemplate"]}],


  "scaled": {
       "mras":[{
           "mraSystemConfig":{"name":"MRA1-1"},
            "associatedMpes":[{"mpeName":"MPE1-1-2"}]
               }],
       "mpes":[{
    "mpeSystemConfig":{"name":"MPE1-1-2"},
            "mpeConfig":{"diameterIdentity":"mpe112",
                       "diameterRealm":"oracle.com"},
            "associatedTemplates":["mpeTemplate"]
            }]
          }
}
```

3.4.3.3 Template Mapping File

The CMP/NF Agent also uses a file called the Template Mapping file to associate scaling levels with Service Configuration files. The template mapping file is located at `/opt/camiant/vnfmgr/cfg/poi/TemplateMapping.json`

The template mapping file included in a Policy 12.3 system looks like this:

```
{
  "deployTemplateMapping": {
     "1":"OCPM_Topology_ServiceConfig_1",
     "2":"OCPM_Topology_ServiceConfig_2",
     "3":"OCPM_Topology_ServiceConfig_3"
                           },
  "scalOutTemplateMapping": {
     "1":"OCPM_Topology_ServiceConfig_1",
     "2":"OCPM_Topology_ServiceConfig_2",
     "3":"OCPM_Topology_ServiceConfig_3"
                           },
"scalInTemplateMapping": {
     "0":"OCPM_Topology_ServiceConfig_1",
     "1":"OCPM_Topology_ServiceConfig_2",
     "2":"OCPM_Topology_ServiceConfig_3"
                           }
}
```

3.4.3.4 Policy Orchestration Adapter (POA) Interface

Communication between an orchestrator and the NF Agent is accomplished using a RESTful API called the Policy Orchestration Adapter (POA) interface.

POA allows these actions to be sent to the NF Agent:

- Active: sent to CMP servers to determine the Active CMP server

```
GET http://<cmp_ip>:80/vnfadapter/nsoapi/v2/topology/active
```

- Template: sends a request to Active CMP server to retrieve a Heat template

```
GET http://<cmp_ip>:80/vnfadapter/nsoapi/v2/topology/template/{level}
```

- Instantiation: sends a Heat template to Active CMP server requesting a deployment

```
POST http://<cmp_ip>:80/vnfadapter/nsoapi/v2/topology/instantiation
```

- Scale: sends a Heat template to Active CMP server requesting a scale in or scale out

```
POST http://<cmp_ip>:80/vnfadapter/nsoapi/v2/topology/scale
```

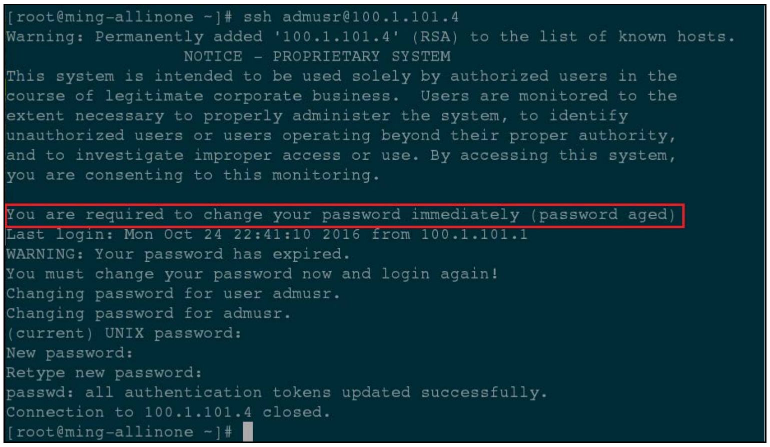
3.5 Password Expiration Time Must Be Implemented (60 days) (PR 24522459)

3.5.1 Introduction

This is an existing general feature in Policy Management.

For the OS level accounts, password expiration forces a password change during the login process when the current password has expired (depicted in Figure 1 and Figure 2), even the SSH authorized keys have been provisioned correctly.

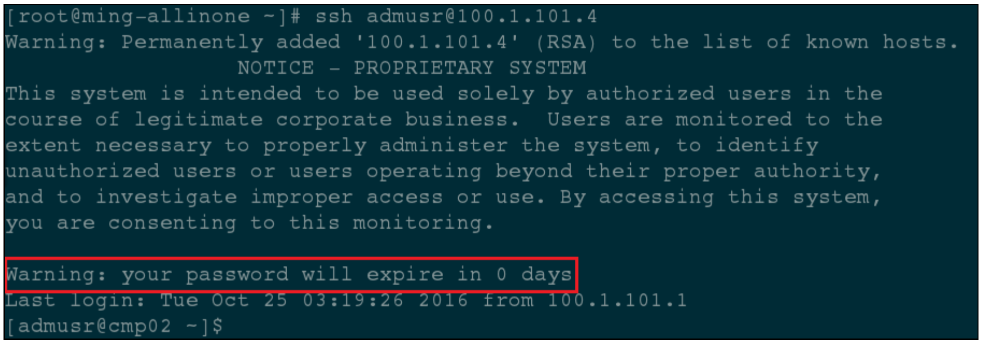
Figure 7 Password Expired for OS Account



```
[root@ming-allinone ~]# ssh admusr@100.1.101.4
Warning: Permanently added '100.1.101.4' (RSA) to the list of known hosts.
                  NOTICE - PROPRIETARY SYSTEM
This system is intended to be used solely by authorized users in the
course of legitimate corporate business.  Users are monitored to the
extent necessary to properly administer the system, to identify
unauthorized users or users operating beyond their proper authority,
and to investigate improper access or use. By accessing this system,
you are consenting to this monitoring.

You are required to change your password immediately (password aged)
Last login: Mon Oct 24 22:41:10 2016 from 100.1.101.1
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user admusr.
Changing password for admusr.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Connection to 100.1.101.4 closed.
[root@ming-allinone ~]#
```

Figure 8 Warning before Password Expiration



```
[root@ming-allinone ~]# ssh admusr@100.1.101.4
Warning: Permanently added '100.1.101.4' (RSA) to the list of known hosts.
                  NOTICE - PROPRIETARY SYSTEM
This system is intended to be used solely by authorized users in the
course of legitimate corporate business.  Users are monitored to the
extent necessary to properly administer the system, to identify
unauthorized users or users operating beyond their proper authority,
and to investigate improper access or use. By accessing this system,
you are consenting to this monitoring.

Warning: your password will expire in 0 days
Last login: Tue Oct 25 03:19:26 2016 from 100.1.101.1
[admusr@cmp02 ~]$
```

3.5.2 Detailed Description

Two password expiration parameters can be configured:

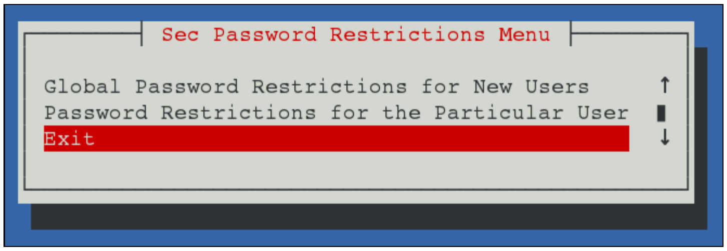
- P1: Maximum number of days a password may be used
- P2: Number of days a user is warned before password expiration

This configuration is performed on each server in the topology.

- P2 is an integer which is greater than or equal to 0.
- P1 is an integer which is greater than 0.
- P2 must be less than or equal to P1.
- The maximum value of P1 is 99999.
- There is no forcibly check in the platcfg utility for the maximum value.

In the Security menu in top menu list of the platcfg utility for such configuration, there are two sub menu items under the Sec Password Restrictions menu:

Figure 9 Sec Password Restrictions Menu


Sec Password Restrictions Menu
Global Password Restrictions for New Users
Password Restrictions for the Particular User
Exit

Global Password Restrictions for New Users is used to set the default password expiration parameters for new OS accounts.

Internally, these configuration keys in the `/etc/login.defs` file update accordingly:

- PASS_MAX_DAYS: Maximum number of days a password can be used
- PASS_WARN_AGE: Number of days a user is warned before password expiration

Password Restrictions for the Particular User is used to set the password expiration parameters for an existing OS account. Therefore, you must provide the target account name and password. Internally, the record of this account is in the `/etc/shadow` file and is updated accordingly.

Minimum acceptable size of for new password and **Minimum number of days allowed between password changes** are not included in this document. In most cases, these parameters remain unchanged.

3.5.2.1 Limitation

A limitation is that the default values in the particular user menu does not reflect the real values. They are only default values in the GUI. In other words, you must input the expected value for each field in the menu. Otherwise, the default value in the GUI overwrites the real value.

Example: For admusr, **Maximum number of days a password may be used** is set to 60. Then when you open the menu, you find that the value of **Maximum number of days a password may be used** is still 90, the GUI default value. When you change another field **Number of days a user is warned before password expiration**, and click **OK**, the **Maximum number of days a password may be used** is also set to 90.

3.5.3 User Interface Changes

No Changes

3.6 Permits in Files Implemented So Only Property of Root (PR 24522481)

3.6.1 Introduction

An upgrade/installation initialization script should be able to automatically remove world-readable access permission from these files in an upgrade.

- `/etc/inittab`
- `/etc/hosts.deny`
- `/etc/hosts.allow`
- `/etc/fstab`

The access mode of these files are:

- `-rw-------  /etc/inittab`
- `-rw-r-----  /etc/hosts.deny`
- `-rw-r-----  /etc/hosts.allow`
- `-rw-r-----  /etc/fstab`

3.6.2 Detailed Description

In an upgrade/installation, a server reboots.

A new QP initialization script `/opt/camiant/bin/upgrade/initializeAccessMode` is called through `/etc/rc4.d/S69zQPLateInit` when the server first reboots.

In this initialization script, **`chmod o-r`** is run for the files.

Backout reverts the access mode of the files to the status before upgrade.

3.6.3 User Interface Changes

No Changes

3.7 Security Certificate of the SSL/TLS Current and Valid (PR 24522484)

3.7.1 Introduction

This is an existing general feature in Policy Management. The configuration procedures are consolidated and updated.

3.7.2 Detailed Description

The configuration of SSL certificates are used to encrypt two kinds of connections:

1. Connections over Management Interface (MI) between CMP and Policy Server.
2. Connections between NW-CMP and S-CMP in multi-OAM Policy Management deployment.

The procedures are described in details for SSL certificate configuration in the Policy Management documentation.

- Procedure 1. Create/Refresh self-signed certificate.
- Procedure 2. Export and import certificate (existing method)
- Procedure 3. Export certificate to CMP with helper tool (new method)
- Procedure 4. Enable/disable secure connection on CMP/S-CMP GUI.
- Procedure 5. Enable/disable secure connection on NW-CMP GUI.

Procedure 2 and procedure 3 are for same purpose with regard to exporting a certificate from Policy Server to CMP. The difference is that procedure 2 is performed on each Policy Server cluster and the primary active CMP server, while procedure 3 is only performed on the primary active CMP server once.

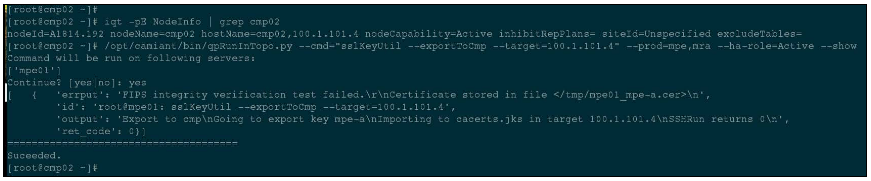
This saves time, as there may be dozens of Policy Server clusters. But the limitation of procedure 3 is that there should be only one certificate in the local keystore for the Policy Server.

Procedure 3 is not applicable to SSL certificate configuration for connections between NW-CMP and S-CMP. In other words, you have to use procedure 2 for the configuration between NW-CMP and S-CMP.

3.7.3 User Interface Changes

3.7.3.1 Procedure 3. Export Certificate to CMP with Helper Tool

Task	Procedure

Export and import centrally.	1. Run this command to switch to root:
	`sudo su -`
	2. Run this command:
	`/opt/camiant/bin/qpRunInTopo.py --cmd=”sslKeyUtil --exportToCmp --target=<OAM_Blade_IP_of_Primary_Active_CMP>” --pool-size=1 --prod=mpe,mra --ha-role=Active [--show]`
	Example:
	
	`[root@cmp02 ~]#`
	`[root@cmp02 ~]# iqt -pE NodeInfo | grep cmp02`
	`nodeId=A1814.192 nodeName=cmp02 hostName=cmp02,100.1.101.4 nodeCapability=Active inhibitRepPlans= siteId=Unspecified excludeTables=`
	`[root@cmp02 ~]# /opt/camiant/bin/qpRunInTopo.py --cmd="sslKeyUtil --exportToCmp --target=100.1.101.4" --prod=mpe,mra --ha-role=Active --show`
	`Command will be run on following servers:`
	`['mpe01']`
	`Continue? [yes|no]: yes`
	`[   {   'errput': 'FIPS integrity verification test failed.\r\nCertificate stored in file </tmp/mpe01_mpe-a.cer>\n',`
	`        'id': 'root@mpe01: sslKeyUtil --exportToCmp --target=100.1.101.4',`
	`        'output': 'Export to cmp\nGoing to export key mpe-a\nImporting to cacerts.jks in target 100.1.101.4\nSSHRun returns 0\n',`
	`        'ret_code': 0}]`
	`======================================`
	`Suceeded.`
	`[root@cmp02 ~]#`
	`--show` is optional. With this option, the details are printed.
	`sslKeyUtil` is a tool run on the active server in each MPE/MRA cluster. It:
	• Exports certificate from local keystore to a local file.
	• Copies the file to CMP server specified in –target.
	• Imports the file into certificate keystore on the CMP server.

3.8 Time Conditional ARP and QCI (PR 24750030)

3.8.1 Introduction

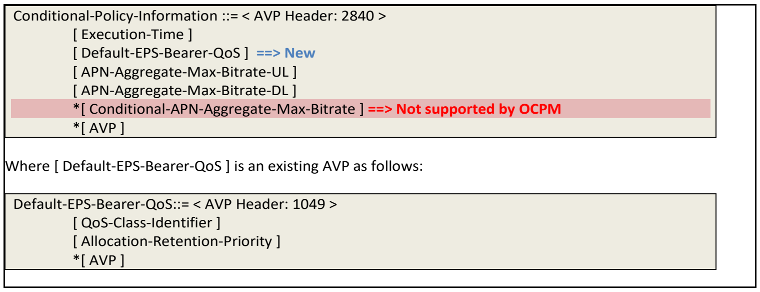
This feature reduces the network congestion which is resulted from a large number of simultaneous APN-AMBR Default-EPS-Bearer-QoS value changes. The operator has requested the ability to set ARP and QCI at a specified time.

This enhancement extends the Conditional-Policy-Info AVP [Time-Conditioned APN-AMBR] to include ARP and QCI information. Specifically, the existing Default-EPS-Bearer-QoS (DEBQ) AVP is optionally added into the Conditional-Policy-Information grouped AVP. This feature also supports a way to synchronize Execution time and rule Activation time when randomization is used.

3.8.2 Detailed Description

The AVPs added to support this feature enhancement are:

- [Execution-Time]
- [Conditional-Policy-Information]



```
Conditional-Policy-Information ::= < AVP Header: 2840 >
            [ Execution-Time ]
            [ Default-EPS-Bearer-QoS ]  ==> New
            [ APN-Aggregate-Max-Bitrate-UL ]
            [ APN-Aggregate-Max-Bitrate-DL ]
            *[ Conditional-APN-Aggregate-Max-Bitrate ] ==> Not supported by OCPM
            *[ AVP ]

Where [ Default-EPS-Bearer-QoS ] is an existing AVP as follows:

Default-EPS-Bearer-QoS::= < AVP Header: 1049 >
            [ QoS-Class-Identifier ]
            [ Allocation-Retention-Priority ]
            *[ AVP ]
```

The contents of Conditional-Policy-Information AVP depend on the features that are enabled. Table 4 shows the support of APN-AMBR and DEBQ in Conditional-Policy-Information AVP with respect to new features.

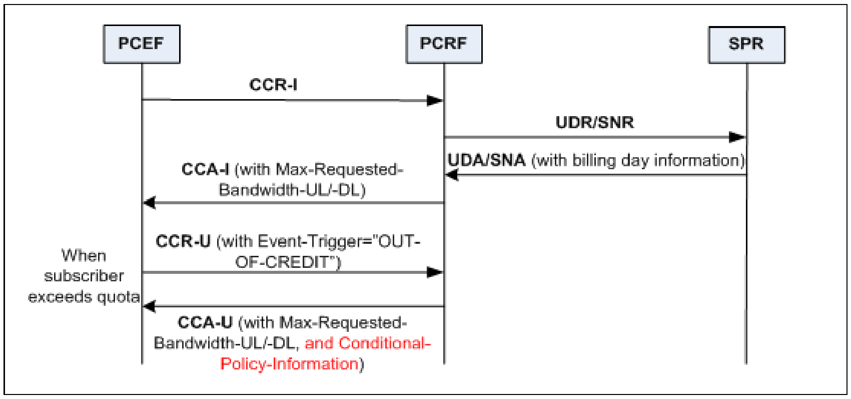
Table 4 Support of APN-AMBR and DEBQ in Conditional-Policy-Information AVP

CondPolicyInfo	CondPolicyInfo-DefaultQoS	APN-AMBR-UL/DL	Default-EPS-Bearer-QoS (DEBQ)
Enabled	Enabled	Supported	Supported
Disabled	Enabled	Not Supported	Supported
Enabled	Disabled	Supported	Not Supported
Disabled	Disabled	Not Supported	Not Supported

With this enhancement, Policy Management can specify when APN-AMBR/DEBQ values should be reset to their non-throttled values in the same message which initiates the throttling.

Figure 8 shows the call flow using Condition-Policy-Information AVP.

Figure 10 Call Flow Using Condition-Policy-Information AVP

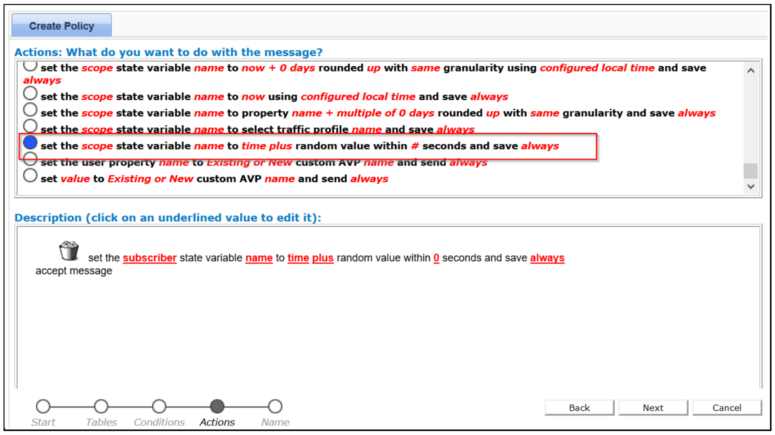

PCEF
PCRF
SPR
CCR-I
UDR/SNR
UDA/SNA (with billing day information)
CCA-I (with Max-Requested-Bandwidth-UL/-DL)
CCR-U (with Event-Trigger="OUT-OF-CREDIT")
When subscriber exceeds quota
CCA-U (with Max-Requested-Bandwidth-UL/-DL, and Conditional-Policy-Information)

1. The PCEF sends a CCR-initial to the PCRF.
2. The PCRF sends a UDR to the SPR to lookup the profile and quota records for the user.
3. The SPR sends a UDA containing the profile and quota records for the user.
4. The PCRF sends a CCA-initial to the PCEF containing APN-AMBR-UL/-DL for that user.
5. The PCEF sends CCR-Update message with Event-Trigger set to OUT_OF_CREDIT(15) when subscriber exhausts his quota at this instance his APN-AMBR-UL/-DL/DEBQ is throttled.
6. CCA-U is sent from PCRF with throttled values of APN-AMBR-UL/DL, DEBQ along with Conditional-policy-Information AVP with un-throttled values of APN-AMBR-UL/-DL/DEBQ and Execution-Time set to a time after which PCEF must enforce these un-throttled values to the subscriber.

3.8.3 User Interface Changes

These GUI screens show the two new policy actions (optional policy actions) added/modified as part of this this enhancement.

First policy action to set a state variable is added under **POLICY MANAGEMENT → Policy Library → Create Policy → Actions**


Create Policy

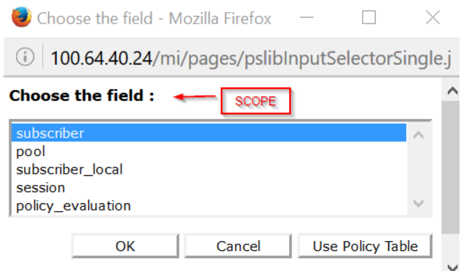
Actions: What do you want to do with the message?

○ set the *scope* state variable *name* to *now + 0 days* rounded *up* with *same* granularity using *configured local time* and save *always*
○ set the *scope* state variable *name* to *now* using *configured local time* and save *always*
○ set the *scope* state variable *name* to property *name + multiple of 0 days* rounded *up* with *same* granularity and save *always*
○ set the *scope* state variable *name* to select traffic profile *name* and save *always*
● set the *scope* state variable *name* to *time plus* random value within *#* seconds and save *always*
○ set the user property *name* to *Existing or New* custom AVP *name* and send *always*
○ set *value* to *Existing or New* custom AVP *name* and send *always*

Description (click on an underlined value to edit it):

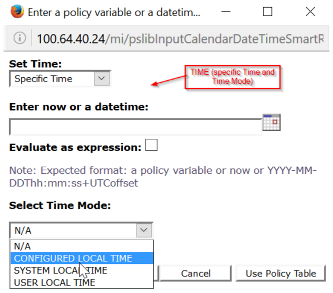
set the subscriber state variable name to time plus random value within 0 seconds and save always
accept message

The GUI screens to configure fields for the policy action:


Choose the field - Mozilla Firefox
100.64.40.24/mi/pages/pslibInputSelectorSingle.j
SCOPE
OK
Cancel
Use Policy Table

Choose the field :

subscriber
pool
subscriber_local
session
policy_evaluation


Enter a policy variable or a datetim...
100.64.40.24/mi/pslibInputCalendarDateTimeSmartR
TIME (specific Time and Time Mode)
Cancel
Use Policy Table

Set Time: Specific Time

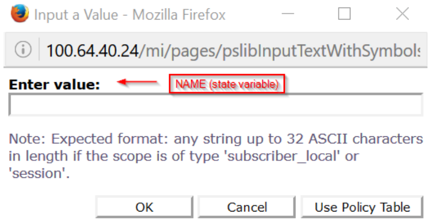
Enter now or a datetime:

Evaluate as expression: □

Note: Expected format: a policy variable or now or YYYY-MM-DDThh:mm:ss+UTCoffset

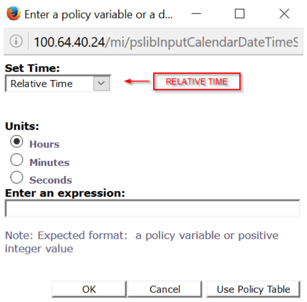
Select Time Mode: N/A

N/A
CONFIGURED LOCAL TIME
SYSTEM LOCAL TIME
USER LOCAL TIME


Input a Value - Mozilla Firefox
100.64.40.24/mi/pages/pslibInputTextWithSymbol:
NAME (state variable)
OK
Cancel
Use Policy Table

Enter value:

Note: Expected format: any string up to 32 ASCII characters in length if the scope is of type 'subscriber_local' or 'session'.

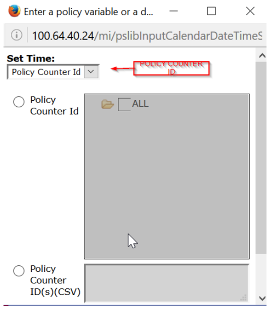

Enter a policy variable or a d...
100.64.40.24/mi/pslibInputCalendarDateTimeS
RELATIVE TIME
OK
Cancel
Use Policy Table

Set Time: Relative Time

Units:
● Hours
○ Minutes
○ Seconds

Enter an expression:

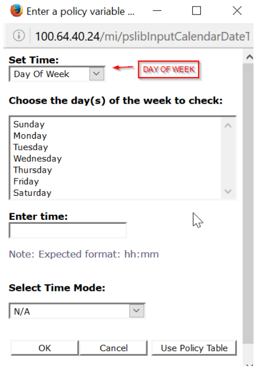
Note: Expected format: a policy variable or positive integer value


Enter a policy variable or a d...
100.64.40.24/mi/pslibInputCalendarDateTimeS
POLICY COUNTER ID

Set Time: Policy Counter Id

○ Policy Counter Id □ ALL

○ Policy Counter ID(s)(CSV)


Enter a policy variable ...
100.64.40.24/mi/pslibInputCalendarDateT
DAY OF WEEK
OK
Cancel
Use Policy Table

Set Time: Day Of Week

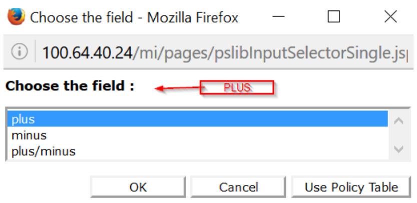
Choose the day(s) of the week to check:

Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

Enter time:

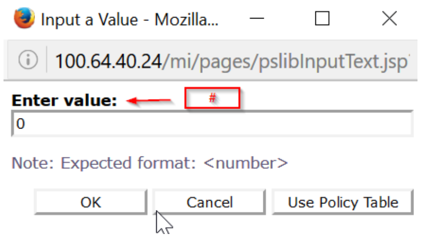
Note: Expected format: hh:mm

Select Time Mode: N/A


Choose the field - Mozilla Firefox
100.64.40.24/mi/pages/pslibInputSelectorSingle.jsp
PLUS
OK
Cancel
Use Policy Table

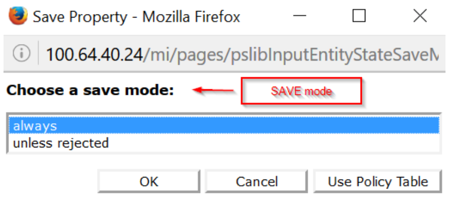
Choose the field :

plus
minus
plus/minus


Input a Value - Mozilla...
100.64.40.24/mi/pages/pslibInputText.jsp
#
OK
Cancel
Use Policy Table

Enter value: 0

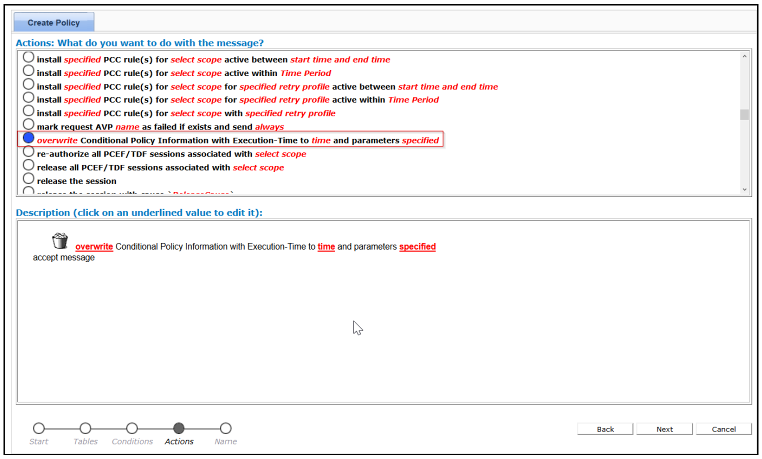
Note: Expected format: <number>


Save Property - Mozilla Firefox
100.64.40.24/mi/pages/pslibInputEntityStateSaveM
SAVE mode
OK
Cancel
Use Policy Table

Choose a save mode:

always
unless rejected

Second policy action to set a Conditional-Policy-Information AVP is added under **POLICY MANAGEMENT → Policy Library → Create Policy → Actions**



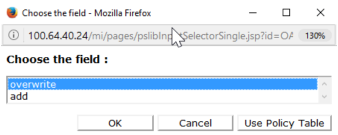
Actions: What do you want to do with the message?

○ install *specified* PCC rule(s) for *select scope* active between *start time and end time*
○ install *specified* PCC rule(s) for *select scope* active within *Time Period*
○ install *specified* PCC rule(s) for *select scope* for *specified retry profile* active between *start time and end time*
○ install *specified* PCC rule(s) for *select scope* for *specified retry profile* active within *Time Period*
○ install *specified* PCC rule(s) for *select scope* with *specified retry profile*
○ mark request AVP *name* as failed if exists and send *always*
● *overwrite* Conditional Policy Information with Execution-Time to *time* and parameters *specified*
○ re-authorize all PCEF/TDF sessions associated with *select scope*
○ release all PCEF/TDF sessions associated with *select scope*
○ release the session

Description (click on an underlined value to edit it):

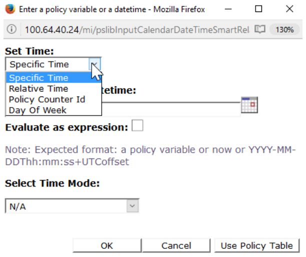
overwrite Conditional Policy Information with Execution-Time to time and parameters specified
accept message

The GUI screens to configure the fields in the policy action are:


Choose the field - Mozilla Firefox
100.64.40.24/mi/pages/pslibInp SelectorSingle.jsp?id=OA
130%
OK
Cancel
Use Policy Table

Choose the field :

overwrite
add


Enter a policy variable or a datetime - Mozilla Firefox
100.64.40.24/mi/pslibInputCalendarDateTimeSmartRel
130%
OK
Cancel
Use Policy Table

Set Time: Specific Time

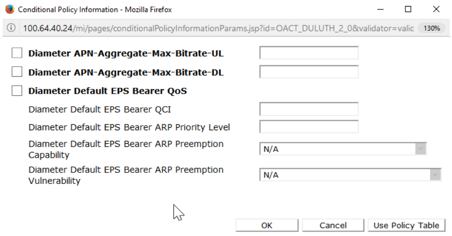
Specific Time
Relative Time
Policy Counter Id
Day Of Week

etime:

Evaluate as expression: □

Note: Expected format: a policy variable or now or YYYY-MM-DDThh:mm:ss+UTCoffset

Select Time Mode: N/A


Conditional Policy Information - Mozilla Firefox
100.64.40.24/mi/pages/conditionalPolicyInformationParams.jsp?id=OACT_DULUTH_2_0&validator=valid
130%
OK
Cancel
Use Policy Table

□ Diameter APN-Aggregate-Max-Bitrate-UL

□ Diameter APN-Aggregate-Max-Bitrate-DL

□ Diameter Default EPS Bearer QoS

Diameter Default EPS Bearer QCI

Diameter Default EPS Bearer ARP Priority Level

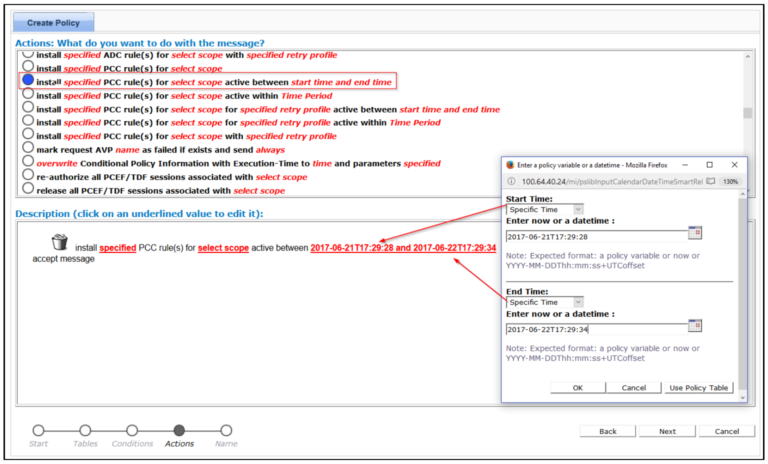
Diameter Default EPS Bearer ARP Preemption Capability: N/A

Diameter Default EPS Bearer ARP Preemption Vulnerability: N/A

Modified policy actions (1):

```
install specified PCC rule(s) for select scope active between start time and end time.
```

Install PCC rules with activation and deactivation time; under **POLICY MANAGEMENT → Policy Library→ Create Policy → Actions**


Create Policy
Enter a policy variable or a datetime - Mozilla Firefox
100.64.40.24/mi/pslibInputCalendarDateTimeSmartRel
130%
OK
Cancel
Use Policy Table
Start
Tables
Conditions
Actions
Name
Back
Next
Cancel

Actions: What do you want to do with the message?

○ install *specified* ADC rule(s) for *select scope* with *specified retry profile*
○ install *specified* PCC rule(s) for *select scope*
● install *specified* PCC rule(s) for *select scope* active between *start time and end time*
○ install *specified* PCC rule(s) for *select scope* active within *Time Period*
○ install *specified* PCC rule(s) for *select scope* for *specified retry profile* active between *start time and end time*
○ install *specified* PCC rule(s) for *select scope* for *specified retry profile* active within *Time Period*
○ install *specified* PCC rule(s) for *select scope* with *specified retry profile*
○ mark request AVP *name* as failed if exists and send *always*
○ *overwrite* Conditional Policy Information with Execution-Time to *time* and parameters *specified*
○ re-authorize all PCEF/TDF sessions associated with *select scope*
○ release all PCEF/TDF sessions associated with *select scope*

Description (click on an underlined value to edit it):

install specified PCC rule(s) for select scope active between 2017-06-21T17:29:28 and 2017-06-22T17:29:34
accept message

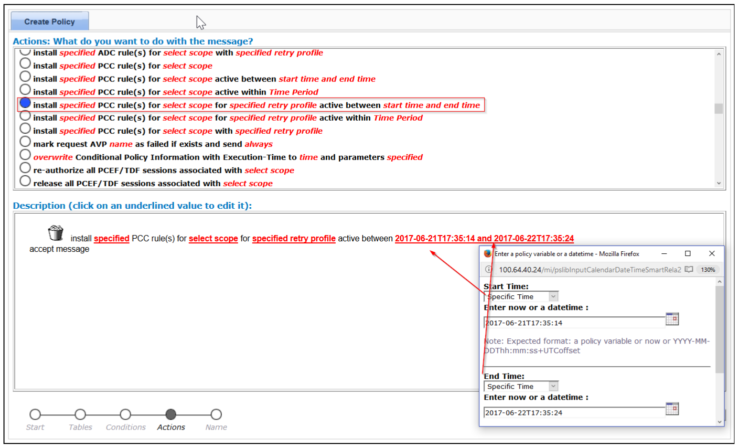
Start Time: Specific Time
Enter now or a datetime : 2017-06-21T17:29:28
Note: Expected format: a policy variable or now or YYYY-MM-DDThh:mm:ss+UTCoffset

End Time: Specific Time
Enter now or a datetime : 2017-06-22T17:29:34
Note: Expected format: a policy variable or now or YYYY-MM-DDThh:mm:ss+UTCoffset

Modified policy actions (2):

```
install specified PCC rule(s) for select scope for specified retry profile active between start time and end time
```

Install PCC rules with activation and deactivation time with a retry profile; under **POLICY MANAGEMENT → Policy Library → Create Policy → Actions**


Create Policy
Enter a policy variable or a datetime - Mozilla Firefox
100.64.40.24/mi/pslibInputCalendarDateTimeSmartRela2
130%
Start
Tables
Conditions
Actions
Name

Actions: What do you want to do with the message?

○ install *specified* ADC rule(s) for *select scope* with *specified retry profile*
○ install *specified* PCC rule(s) for *select scope*
○ install *specified* PCC rule(s) for *select scope* active between *start time and end time*
○ install *specified* PCC rule(s) for *select scope* active within *Time Period*
● install *specified* PCC rule(s) for *select scope* for *specified retry profile* active between *start time and end time*
○ install *specified* PCC rule(s) for *select scope* for *specified retry profile* active within *Time Period*
○ install *specified* PCC rule(s) for *select scope* with *specified retry profile*
○ mark request AVP *name* as failed if exists and send *always*
○ *overwrite* Conditional Policy Information with Execution-Time to *time* and parameters *specified*
○ re-authorize all PCEF/TDF sessions associated with *select scope*
○ release all PCEF/TDF sessions associated with *select scope*

Description (click on an underlined value to edit it):

install specified PCC rule(s) for select scope for specified retry profile active between 2017-06-21T17:35:14 and 2017-06-22T17:35:24
accept message

Start Time: Specific Time
Enter now or a datetime : 2017-06-21T17:35:14
Note: Expected format: a policy variable or now or YYYY-MM-DDThh:mm:ss+UTCoffset

End Time: Specific Time
Enter now or a datetime : 2017-06-22T17:35:24

As part of the modified policy action, this field is modified:

`start time and end time`: This field can be configured using a drop down which allows you to select specific time, relative time, or Policy Counter ID. Currently (before this feature), Specific Time did not support Policy variable substitution. As part of this feature, specific time supports Policy variable substitution.

Other fields are unchanged.

3.9 MRA Associations Backup and Restore (PR 20162817)

3.9.1 Introduction

CMP allows you to export/import (via GUI and OSSI) checkpoint information which allows you to recreate the deployed MRA Associations, including Client Mapping Tables (PCD configuration).

3.9.2 Detailed Description

This feature enhances the existing supported OSSI function by adding the XML OSSI request types:

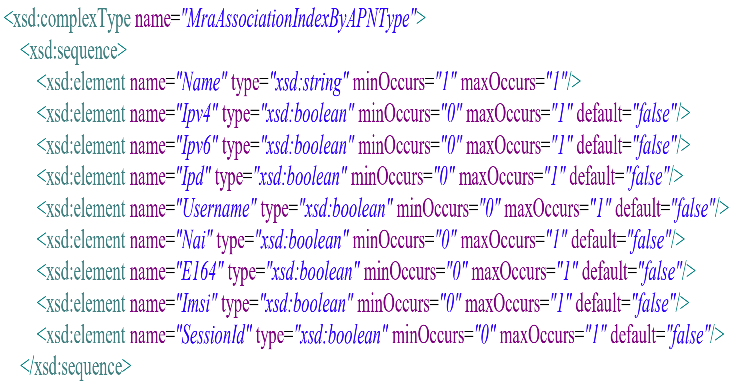
- AddMraAssociation
- UpdateMraAssociation
- DeleteMraAssociation
- QueryMraAssociation

The Import/Export and check point functions only use AddMraAssociation.

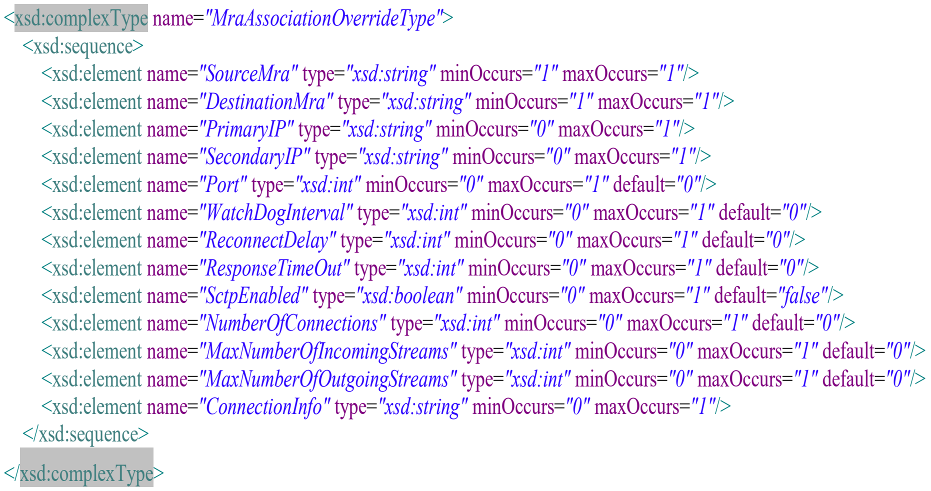
These example show the general format of the added OSSI XML request types defined in `export.xsd` file.

```
<xsd:complexType name="MraAssociationType">
  <xsd:sequence>
    <xsd:element name="Name" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Description" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="Type" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="PrimaryIndex" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="IndexByUsername" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="IndexByNai" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="IndexByE164" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="IndexByAddressV4" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="IndexByIPD" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="IndexByImsi" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="IndexBySessionId" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="IndexByAddressV6" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="Member" type="MraAssociationMemberType" minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="Override" type="MraAssociationOverrideType" minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="IndexByAPN" type="MraAssociationIndexByAPNType" minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="PCD" type="MraAssociationPCDType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

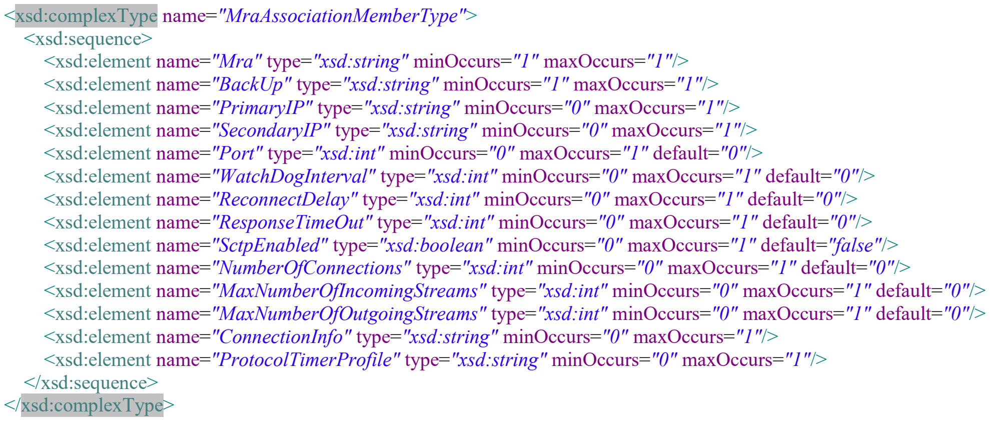
```
<xsd:complexType name="UpdateMraAssociationType">
    <xsd:sequence>
        <xsd:element name="Name" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="Description" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="Type" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="PrimaryIndex" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="IndexByUsername" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="IndexByNai" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="IndexByE164" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="IndexByAddressV4" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="IndexByIPD" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="IndexByImsi" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="IndexBySessionId" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="IndexByAddressV6" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="Member" type="UpdateMraAssociationMemberType" minOccurs="0" maxOccurs="unbounded"/>
        <xsd:element name="Override" type="UpdateMraAssociationOverrideType" minOccurs="0" maxOccurs="unbounded"/>
        <xsd:element name="IndexByAPN" type="UpdateMraAssociationIndexByAPNType" minOccurs="0" maxOccurs="unbounded"/>
        <xsd:element name="PCD" type="UpdateMraAssociationPCDType" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>
```



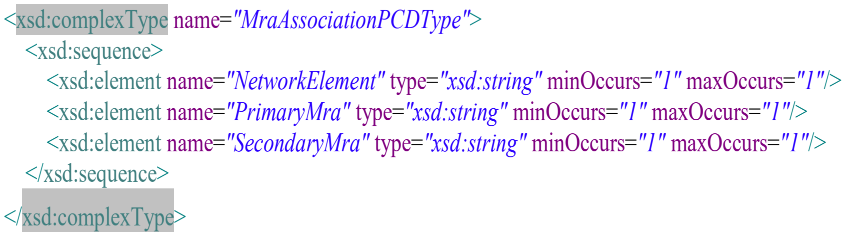
```
<xsd:complexType name="MraAssociationIndexByAPNType">
    <xsd:sequence>
        <xsd:element name="Name" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="Ipv4" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="Ipv6" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="Ipd" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="Username" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="Nai" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="E164" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="Imsi" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="SessionId" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    </xsd:sequence>
```



```
<xsd:complexType name="MraAssociationOverrideType">
    <xsd:sequence>
        <xsd:element name="SourceMra" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="DestinationMra" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="PrimaryIP" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="SecondaryIP" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="Port" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
        <xsd:element name="WatchDogInterval" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
        <xsd:element name="ReconnectDelay" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
        <xsd:element name="ResponseTimeOut" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
        <xsd:element name="SctpEnabled" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
        <xsd:element name="NumberOfConnections" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
        <xsd:element name="MaxNumberOfIncomingStreams" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
        <xsd:element name="MaxNumberOfOutgoingStreams" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
        <xsd:element name="ConnectionInfo" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    </xsd:sequence>
</xsd:complexType>
```



```
<xsd:complexType name="MraAssociationMemberType">
  <xsd:sequence>
    <xsd:element name="Mra" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="BackUp" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="PrimaryIP" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="SecondaryIP" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="Port" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
    <xsd:element name="WatchDogInterval" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
    <xsd:element name="ReconnectDelay" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
    <xsd:element name="ResponseTimeOut" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
    <xsd:element name="SctpEnabled" type="xsd:boolean" minOccurs="0" maxOccurs="1" default="false"/>
    <xsd:element name="NumberOfConnections" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
    <xsd:element name="MaxNumberOfIncomingStreams" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
    <xsd:element name="MaxNumberOfOutgoingStreams" type="xsd:int" minOccurs="0" maxOccurs="1" default="0"/>
    <xsd:element name="ConnectionInfo" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="ProtocolTimerProfile" type="xsd:string" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>
```



```
<xsd:complexType name="MraAssociationPCDType">
  <xsd:sequence>
    <xsd:element name="NetworkElement" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="PrimaryMra" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="SecondaryMra" type="xsd:string" minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>
```

3.9.2.1 Import/Export MRA association

MRA association can be imported/exported from the CMP with the dependency option.

1. In the CMP GUI, navigate to **System Administration → Export → MRA Associations**.
2. Select the MRA associations and add them to the shopping cart with **Include dependency** selected.
3. Switch to shopping cart and export the associations.
4. The fields in the exported file are the same as in the GUI, and the version number in the `exportResult.txt` file shows which version this file is exported from

The configuration package includes:

1. MD5 file
2. Inner zip file that includes:
   - `MRAAssociation.xml`: The MRAAssociation.xml includes MRA associations.
   - `TimerProfile.xml`: The TimerProfile.xml includes timer profiles associated with MRA.
   - `NetworkElements.xml`: The NetworkElements.xml includes network elements associated with MRA.

The TimerProfile.xml and NetworkElements.xml includes timer profiles and network elements associated with MRA.

3.9.2.2 Feature operation failure responses

If there is an error, for example, if referenced objects of a MRA Association in the add/update OSSI request do not exist in the CMP, the MRA Association add/update fails. The reason is in the response message with the associated failure codes.

This is an example of an XML response for operation failure:

```
<?xml version='1.0' ?>
<Response>
```

```
        <Result>0</Result>

        <Command type="XmlInterfaceResponse">

                <Success count="2">Successfully imported 2 MRA Association(s).</Success>

                <Failure count="1">Failed to import 1 MRA Association(s).
ProtocolTimerProfile(protocolTimerProfileTest) not found in Members</Failure>

        </Command>

</Response>
```

3.9.3 User Interface Changes

No Changes

3.10 Policy Management Virtualized Software Bundle (PR 23173988)

3.10.1 Introduction

The Policy Management Virtualized Software Bundle (PMVSB) refers to the ability to deploy a virtualized policy solution (including both Oracle Communications Policy Management and Oracle Communication User Data Repository) with a small capacity footprint, which can facilitate both Policy Management and UDR VMs deployed on a single pair of servers. PMVSB is deployed leveraging the KVM hypervisor on Oracle LINUX operating system. PMVSB can be deployed leveraging any of the 386-based servers that is compatible with the policy solution. Even though PMVSB does not prescribe a specific hardware server configuration, the sizing of the VM profiles has been done to facilitate co-existence of all VMs on a reasonably-equipped pair of servers.

The Policy Management and UDR software releases that are bundled together are managed as independent software releases. The Policy Management and UDR software is deployed leveraging the existing cloud deployment procedures and documentation. Any future maintenance releases and patches can be applied to either application’s VMs independent of the other. The Policy Management and UDR software can be upgraded independently of each other, as long as the combination of Policy Management and UDR releases have been certified to interoperate with each other. Upgrade of the underlying Oracle Linux software requires re-installation of the Policy Management and UDR applications on the upgraded server.

The PMVSB supports all functional use cases that are incorporated into the base Policy Management and UDR releases that are deployed in the bundle. Both the Policy Management and UDR components of the bundle are configured using their corresponding independent OAM interfaces.

3.10.2 Detailed Description

3.10.2.1 VM Resource Allocations

Table 5 outlines the resource allocations for each Policy Management and UDR virtual machine included in the solution. These virtual machines are deployed on the KVM hypervisor (without Openstack) on the Oracle LINUX operating system.

Table 5 Resource Allocations for Each Policy Management and UDR Virtual Machine

Resource Allocation For Policy Management Virtualized Software Bundle					
Product	**Network Element**	**Host Name**	**vCPU Allocation**	**Memory Allocation (GB)**	**Hard Disk Allocation (GB)**
UDR	NO	NO-A	4	48	220
	SO	SO-A	2	4	60
	MP	MP-1	4	16	60
PCRF	CMP	CMP-1	4	10	108
	PFE	PFE-1	10	32	108
	MPE	MPE-1	10	32	108
	MPE	MPE-2	10	32	108
PlatMgmt	KVM		2	2	154
Required Resource Count			46	176	926

3.10.2.2 Networking

A single Diameter signaling network is shared by both the Policy Management and UDR applications. This network is used for all Diameter traffic between the Policy Management and your network, as well as the Sh Diameter traffic between the Policy Management MPE and the UDR MPs.

A single OAM network is shared by both Policy Management and UDR. In general, Policy Management and UDR do not route maintenance traffic to each other with one exception:

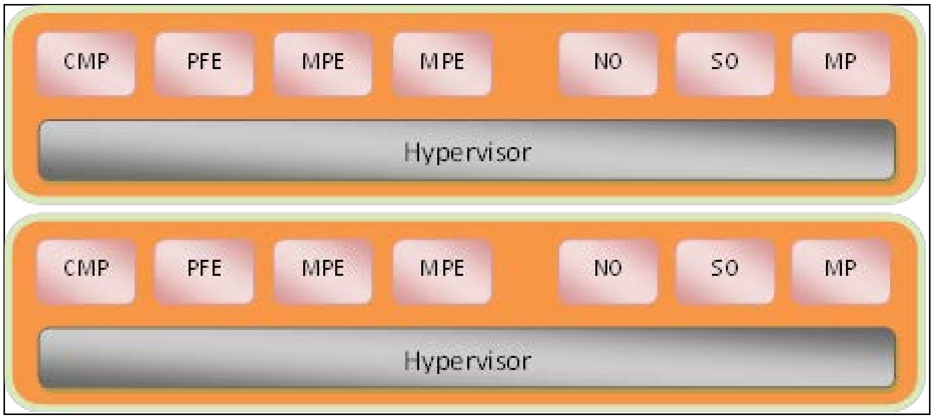
> The CMP GUI can be used to create provisioning requests, which are sent via the external OAM network to UDR.

3.10.2.3 Geo-Diversity/Geo-Redundancy

The Policy Management Virtualized Software Bundle can be deployed either as a single site, or replicated across two sites. A two site configuration consists on deploying an identical configuration at each of two sites.

With a two-site configuration, Policy Management is engineered to be a geo-diverse configuration, through which the solution provides full functional capabilities in the event that the primary site is lost. UDR is engineered to be a georedundant configuration, with all subscriber data fully replicated between the database instances at both sites.

Because this is a geo-diverse Policy Management configuration, session data is not replicated between sites. If the VMs at one site are lost, then sessions are recreated by leveraging the VMs at the surviving site.



3.10.3 User Interface Changes

No Changes

3.11 Revalidation Timer Randomization Feature (PR 22315343)

3.11.1 Introduction

Revalidation Timer Randomization is required to spread out the retries and avoid additional storms of Diameter Messages. This enhancement avoids bursts of CCR-U messages in some cases by allowing you to add a randomization component to policy actions which set the revalidation time.

3.11.2 Detailed Description

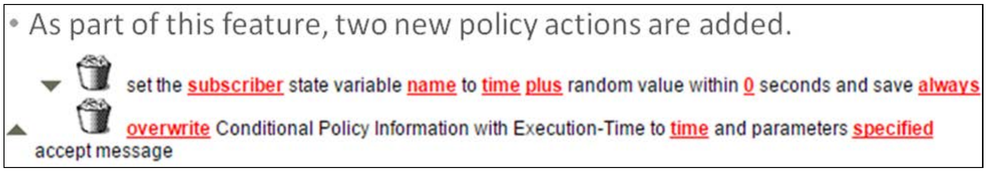
Currently there is not a mechanism to add a random component to timers, that is, Revalidation Timer Randomization.

The feature adds the ability to spread revalidation timer events over a window of time. This can help to alleviate a secondary network congestion event.

Use case (Network Outage/Restoral):

1. Network outage (firewall issue, infrastructure issue, and so on)
2. Network restored resulting in a CCR-I storm to PCRF
3. Sh is still down resulting in no Sh timeout
4. PCRF policy returns the re-validation timer AVP in CCA-I
5. Sh Re-validates are set to about the same time resulting in a potential secondary congestion event.

3.11.3 User Interface Changes



- As part of this feature, two new policy actions are added.

set the subscriber state variable name to time plus random value within 0 seconds and save always

overwrite Conditional Policy Information with Execution-Time to time and parameters specified

accept message

If randomization is required in Execution-Time then, the first user must set the state variable which holds randomized time and then use this variable for setting Execution time. So the configuration order of policy actions matters, that is, the policy action setting the state variable must be configured before using it to set Execution-Time. Therefore, to synchronization across different times such as Execution-Time and Activation time, the same state variable must be used with both.

Example: Randomization of revalidation timer

```
where the event trigger is one of OUT_OF_CREDIT

And where the request is modifying an existing session

set the session state variable StartTimerandVar to 1Hour minus random value within 30 seconds
and save always.

set the session state variable EndTimeRandVar to 2Hour minus random value within 30 seconds and
save always.

add Conditional Policy Information with Execution-Time to {Session.State.StartTimerandVar } and
parameters

Diameter APN-Aggregate-Max-Bitrate-DL              1000

revalidate the session at {Session.State.StartTimerandVar } using CONFIGURED LOCAL TIME.

install pccrule1 PCC rule(s) for session active between {Session.State.StartTimerandVar } and
{Session.State.EndTimeRandVar }.

continue processing message
```

This example illustrates how state variables (`StartTimerandVar, EndTimeRandVar`) can be used in policy actions which set revalidation time and actions which install PCC rules.

3.12 NB-IoT—Cat M2 device support (PR 24953778)

3.12.1 Introduction

This feature enhancement supports the new RAT-TYPE = EUTRAN-NB-IoT (1005)

Policy Management allows you to define policies using the CMP GUI for the EUTRAN-NB-IoT (1005) RAT-type.

Policy Management also allows you to view NB-IoT RAT type specific PDN connection and AF Session Report.

The existing RAT-Type value is used for E-UTRAN and denote WB-E-UTRAN access.

3.12.2 Detailed Description

NB-IoT as access technology to the Access Technology Type Option has been added. However, to distinguish between both E-UTRAN accesses types, the new RAT type value `EUTRAN-NB-IoT (1005)` has been introduced.

Policy Changes

Table 6 outlines the policy changes.

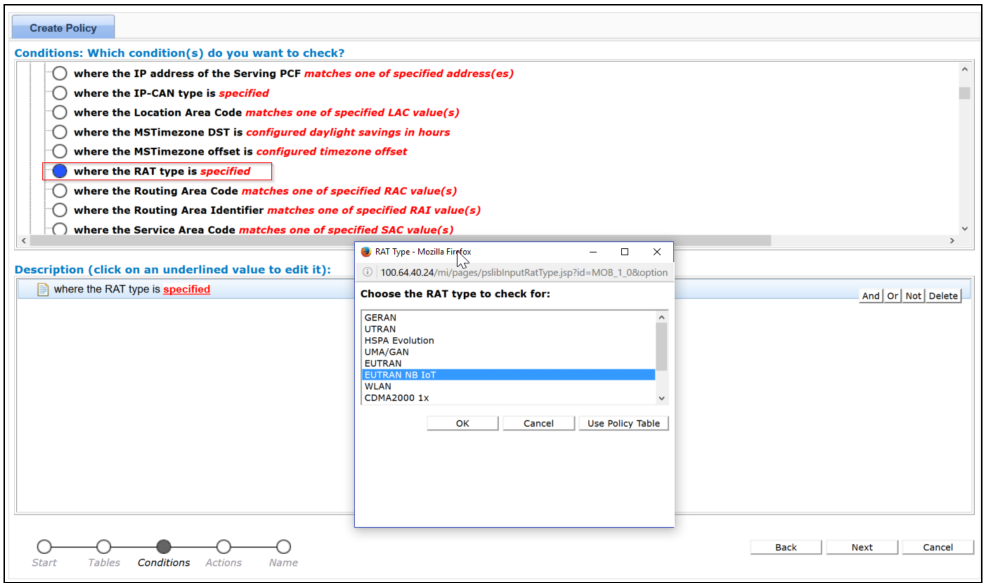
Table 6 Policy Changes for 24953778

Policy Condition Group	Policy Condition or Action	Description
Mobility Conditions	`where the RAT type is` **`specified`**	Check RAT type current date is one of the listed RAT type. Add EUTRAN-NB-IoT (1005) RAT-type in the pull-down list

3.12.3 User Interface Changes

The two new changes made for new RAT type.

For policy, a new menu item **EUTRAN NB IoT** has been added for the mobility RAT type condition under **POLICY MANAGEMENT → Policy Library → Create Policy → Conditions → Mobility → RAT Type** *specified*



Conditions: Which condition(s) do you want to check?

○ where the IP address of the Serving PCF *matches one of specified address(es)*
○ where the IP-CAN type is *specified*
○ where the Location Area Code *matches one of specified LAC value(s)*
○ where the MSTimezone DST is *configured daylight savings in hours*
○ where the MSTimezone offset is *configured timezone offset*
● where the RAT type is *specified*
○ where the Routing Area Code *matches one of specified RAC value(s)*
○ where the Routing Area Identifier *matches one of specified RAI value(s)*
○ where the Service Area Code *matches one of specified SAC value(s)*

Description (click on an underlined value to edit it):

where the RAT type is specified

RAT Type - Mozilla Firefox

100.64.40.24/mi/pages/pslibInputRatType.jsp?id=MOB_1_0&option

Choose the RAT type to check for:

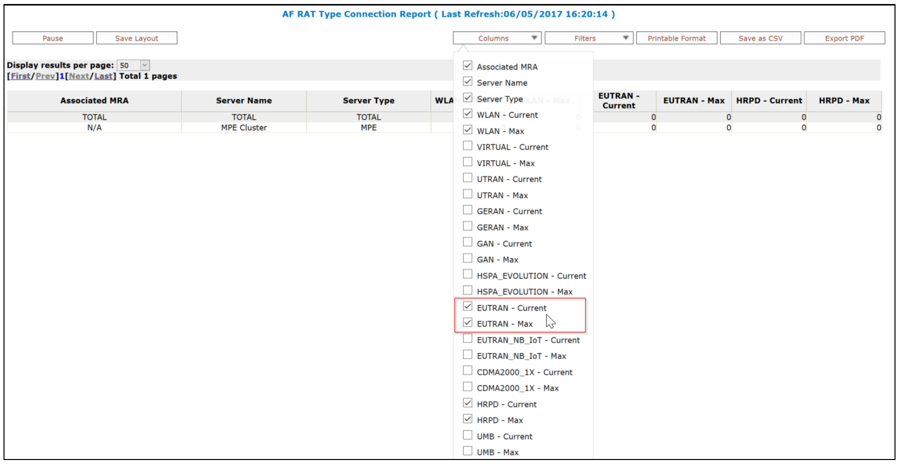
GERAN
UTRAN
HSPA Evolution
UMA/GAN
EUTRAN
EUTRAN NB IoT
WLAN
CDMA2000 1x

The PDN Connection Report and AF Session Report reflect the new RAT type with two additional columns:

- EUTRAN NB IoT
- EUTRAN NB IoT – Current

Figure 11 and Figure 12 outline the AF RAT Type Connection Report and PDN Connection Report for EUTRAN_NB_IOT-Current and EUTRAN_NB_IOT-Max columns.

Figure 11 AF RAT Type Connection Report EUTRAN_NB_IOT-Current and EUTRAN_NB_IOT-Max columns



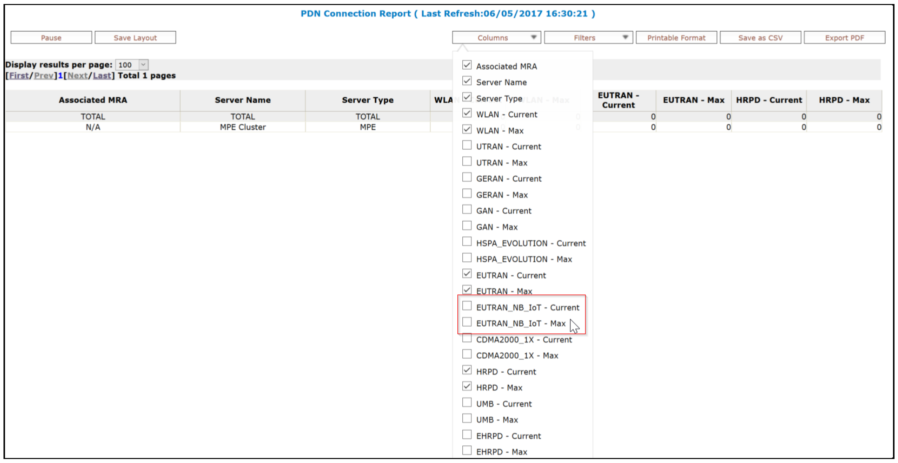
AF RAT Type Connection Report (Last Refresh:06/05/2017 16:20:14)

Display results per page: 50
[First/Prev]1[Next/Last] Total 1 pages

Associated MRA	Server Name	Server Type	WLA	EUTRAN - Current	EUTRAN - Max	HRPD - Current	HRPD - Max
TOTAL	TOTAL	TOTAL		0	0	0	0
N/A	MPE Cluster	MPE		0	0	0	0

☑ Associated MRA
☑ Server Name
☑ Server Type
☑ WLAN - Current
☑ WLAN - Max
□ VIRTUAL - Current
□ VIRTUAL - Max
□ UTRAN - Current
□ UTRAN - Max
□ GERAN - Current
□ GERAN - Max
□ GAN - Current
□ GAN - Max
□ HSPA_EVOLUTION - Current
□ HSPA_EVOLUTION - Max
☑ EUTRAN - Current
☑ EUTRAN - Max
□ EUTRAN_NB_IoT - Current
□ EUTRAN_NB_IoT - Max
□ CDMA2000_1X - Current
□ CDMA2000_1X - Max
☑ HRPD - Current
☑ HRPD - Max
□ UMB - Current
□ UMB - Max

Figure 12 PDN Connection Report for EUTRAN_NB_IOT-Current and EUTRAN_NB_IOT-Max columns



PDN Connection Report (Last Refresh:06/05/2017 16:30:21)

Display results per page: 100
[First/Prev]1[Next/Last] Total 1 pages

Associated MRA	Server Name	Server Type	WLA	EUTRAN - Current	EUTRAN - Max	HRPD - Current	HRPD - Max
TOTAL	TOTAL	TOTAL		0	0	0	0
N/A	MPE Cluster	MPE		0	0	0	0

☑ Associated MRA
☑ Server Name
☑ Server Type
☑ WLAN - Current
☑ WLAN - Max
□ UTRAN - Current
□ UTRAN - Max
□ GERAN - Current
□ GERAN - Max
□ GAN - Current
□ GAN - Max
□ HSPA_EVOLUTION - Current
□ HSPA_EVOLUTION - Max
☑ EUTRAN - Current
☑ EUTRAN - Max
□ EUTRAN_NB_IoT - Current
□ EUTRAN_NB_IoT - Max
□ CDMA2000_1X - Current
□ CDMA2000_1X - Max
☑ HRPD - Current
☑ HRPD - Max
□ UMB - Current
□ UMB - Max
□ EHRPD - Current
□ EHRPD - Max

3.13 MySQL root Password Is Modifiable (PR 25173137)

3.13.1 Introduction

This feature is a requirement of Verizon Wireless in Policy Management R12.3. The requirement asks for that the password of MySQL server must be modifiable. This feature supports the changing MySQL password of root user.

QP (Policy Management Platform) is the manager of MySQL Server and also the manager of root user of MySQL Server. QP sets the password of the root user to default during post fresh-installation phase.

To support changing password of root user, QP takes the role of changing it and supplies CLI to finish this task.

3.13.2 Detailed Description

3.13.2.1 Scope and Role

Table 7 through Table 9 outline the impacted product and component, as well as the role for using root user of MySQL

Table 7 Impacted Product

Product	Note
CMP	CMP has MySQL cluster function and supports GEO redundancy
MA	MA has MySQL cluster function, but does not support GEO redundancy

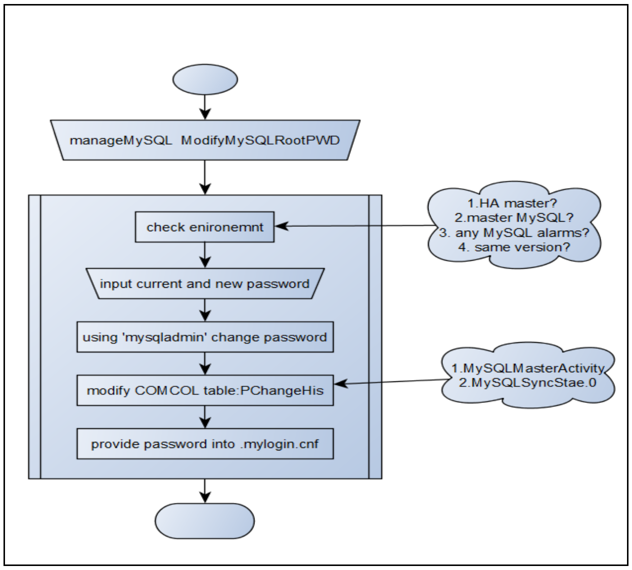
Table 8 Impacted Component

Component	Note
QP	QP uses and operates the root account during IPM, upgrade and product running
APP	APP access MySQL sever in some case by root user, such as create, upgrade and migrate database

Table 9 Role for Using root User of MySQL

Role	Note
User	who use root account to access MySQL Sever, QP and APP both are user
Manager	who manage the root account of MySQL, QP is the manager

3.13.2.2 Procedure to Modify SQL Password


manageMySQL ModifyMySQLRootPWD
check enironemnt
input current and new password
using 'mysqladmin' change password
modify COMCOL table:PChangeHis
provide password into .mylogin.cnf
1.HA master?
2.master MySQL?
3. any MySQL alarms?
4. same version?
1.MySQLMasterActivity
2.MySQLSyncStae.0

1. Check environment

   All of these conditions must be satisfied before you can modify the password:

   a. HA is master

   b. MySQL is master

   c. No MySQL related alarms(70020, 70021, 70022, 70023, 70024, 70025)

   d. For CMP, all servers in current topology have the same release version.

2. Modify password of root in MySQL server

   Because of the MySQL cluster replication, this change is replicated to all slave MySQL, then the password in database of all the MySQL servers is changed synchronously.

3. Update field PChangeHis in COMCOL table MySQLMasterActivity and MySQLSyncState.0 by format timestamp of changing password, encoded string of password

   Because of the COMCOL replication, change in MySQLMasterActivity is synced to all slave MySQL servers.

3.13.2.3 Procedure to Resynchronize Password in MySQL Slave

By a timer event in QP, the MySQL slave triggers the modifying password procedure after detecting the password was changed. Because the password is in the MySQL database, the Server is automatically synced by replication. Modifying the password in the database is not required. Follow this process:

1. If QP detects that PChangeHis in MySQLSyncState.0 is not the same as MySQLMasterActivity, then go to step 2.
2. Update PChangeHis in MySQLSyncState.0 with the password in MySQLMasterActivity.
3. Update the local login path in `.mylogin.cnf` with the new password.

3.13.2.4 Limitations

- Password Length:

  The length is from 1 to 32 characters

- Table 10 outlines whether the new password is retained after a backout.

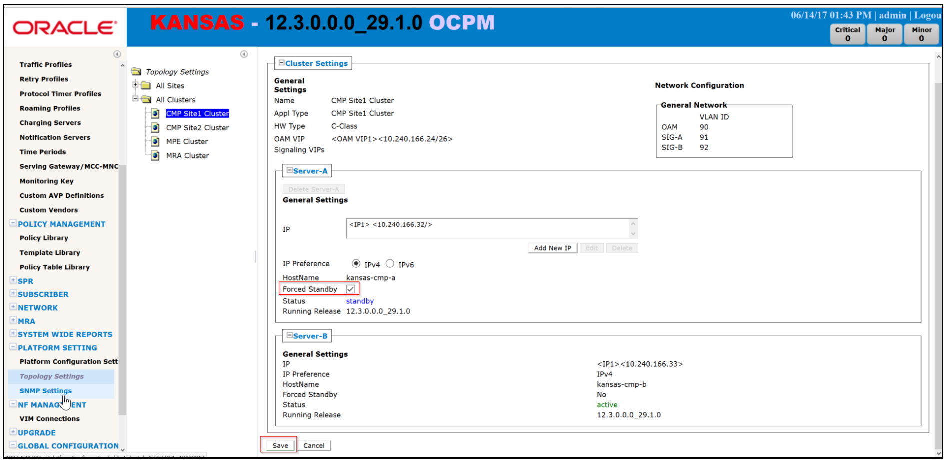
Table 10 Password retention during back out

Base release supports modifying MySQL password	Schema version of base and target release is the same	New password is kept?
No	Yes	No
No	No	No
Yes	**Yes**	**Yes**
Yes	No	No

3.13.3 User Interface Changes

To modify the password of MySQL:

1. Login into CMP GUI to check alarms, if there are no critical alarms and no MySQL related alarms, then go to step 2.
2. Login into CMP GUI, set the slave MySQL node to Forced Standby.



General Settings

Name CMP Site1 Cluster
Appl Type CMP Site1 Cluster
HW Type C-Class
OAM VIP <OAM VIP1><10.240.166.24/26>
Signaling VIPs

Network Configuration

General Network

	VLAN ID
OAM	90
SIG-A	91
SIG-B	92

Server-A

General Settings

IP <IP1> <10.240.166.32/>
IP Preference ● IPv4 ○ IPv6
HostName kansas-cmp-a
Forced Standby ☑
Status standby
Running Release 12.3.0.0.0_29.1.0

Server-B

General Settings

IP <IP1><10.240.166.33>
IP Preference IPv4
HostName kansas-cmp-b
Forced Standby No
Status active
Running Release 12.3.0.0.0_29.1.0

3. Find the master MySQL node

   The master MySQL node is the active MA or CMP in primary site for. There are two ways to find it:

   - Login into CMP GUI, and find the active one in **PlATFORM SETTING→Topology Settings**.
   - Issue the **`wbAccess mysqlState`** command by root user to find the master MySQL(active CMP/MA and active CMP in primary site for GEO topology)

4. On the master, change the password using the CLI command **`manageMySQL ModifyMySQLRootPWD`**

5. Verify the result of modified MySQL root password logs in `/var/camiant/log/qpMySQL.log` file.

   Or

   Issue the **`mysqladmin`** command in server terminal: **`mysqladmin -uroot -p`** <*NewPWD*> **`status`**;

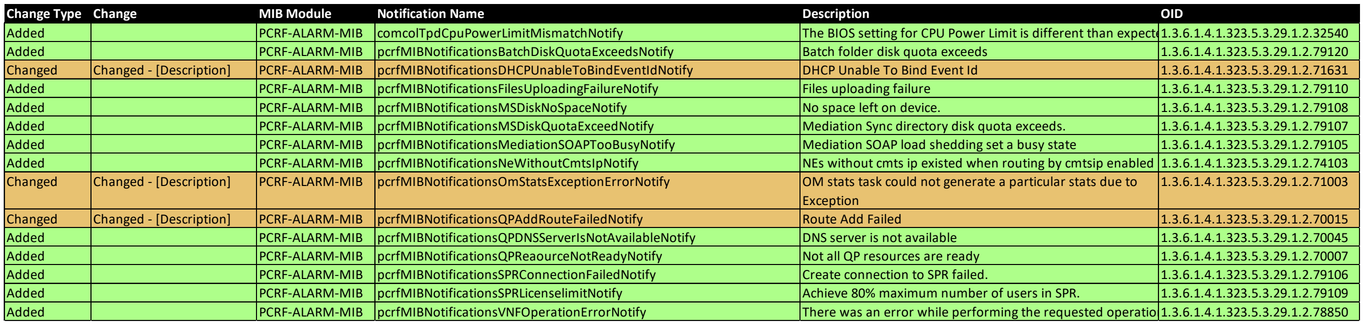
4. PROTOCOL FLOW/PORT CHANGE

No Changes

5. OSSI XML/SNMP MIB CHANGE

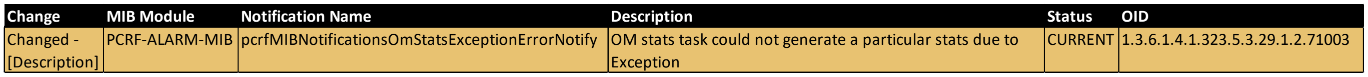
Table 9 through Table 11 list the added, changed and deleted MIB files for the delta of Policy Releases 12.1.x/12.2.x to 12.3.

Table 11 Delta of Changes from Policy 12.1.x to 12.3.x



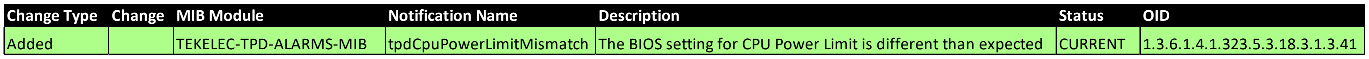
Change Type	Change	MIB Module	Notification Name	Description	OID
Added		PCRF-ALARM-MIB	comcolTpdCpuPowerLimitMismatchNotify	The BIOS setting for CPU Power Limit is different than expect	1.3.6.1.4.1.323.5.3.29.1.2.32540
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsBatchDiskQuotaExceedsNotify	Batch folder disk quota exceeds	1.3.6.1.4.1.323.5.3.29.1.2.79120
Changed	Changed - [Description]	PCRF-ALARM-MIB	pcrfMIBNotificationsDHCPUnableToBindEventIdNotify	DHCP Unable To Bind Event Id	1.3.6.1.4.1.323.5.3.29.1.2.71631
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsFilesUploadingFailureNotify	Files uploading failure	1.3.6.1.4.1.323.5.3.29.1.2.79110
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsMSDiskNoSpaceNotify	No space left on device.	1.3.6.1.4.1.323.5.3.29.1.2.79108
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsMSDiskQuotaExceedNotify	Mediation Sync directory disk quota exceeds.	1.3.6.1.4.1.323.5.3.29.1.2.79107
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsMediationSOAPTooBusyNotify	Mediation SOAP load shedding set a busy state	1.3.6.1.4.1.323.5.3.29.1.2.79105
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsNeWithoutCmtsIpNotify	NEs without cmts ip existed when routing by cmtsip enabled	1.3.6.1.4.1.323.5.3.29.1.2.74103
Changed	Changed - [Description]	PCRF-ALARM-MIB	pcrfMIBNotificationsOmStatsExceptionErrorNotify	OM stats task could not generate a particular stats due to Exception	1.3.6.1.4.1.323.5.3.29.1.2.71003
Changed	Changed - [Description]	PCRF-ALARM-MIB	pcrfMIBNotificationsQPAddRouteFailedNotify	Route Add Failed	1.3.6.1.4.1.323.5.3.29.1.2.70015
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsQPDNSServerIsNotAvailableNotify	DNS server is not available	1.3.6.1.4.1.323.5.3.29.1.2.70045
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsQPReaourceNotReadyNotify	Not all QP resources are ready	1.3.6.1.4.1.323.5.3.29.1.2.70007
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsSPRConnectionFailedNotify	Create connection to SPR failed.	1.3.6.1.4.1.323.5.3.29.1.2.79106
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsSPRLicenselimitNotify	Achieve 80% maximum number of users in SPR.	1.3.6.1.4.1.323.5.3.29.1.2.79109
Added		PCRF-ALARM-MIB	pcrfMIBNotificationsVNFOperationErrorNotify	There was an error while performing the requested operatio	1.3.6.1.4.1.323.5.3.29.1.2.78850

Table 12 Delta of Changes from Policy 12.2.x to 12.3.x



Change	MIB Module	Notification Name	Description	Status	OID
Changed - [Description]	PCRF-ALARM-MIB	pcrfMIBNotificationsOmStatsExceptionErrorNotify	OM stats task could not generate a particular stats due to Exception	CURRENT	1.3.6.1.4.1.323.5.3.29.1.2.71003

Table 13 Delta of TPD Changes from Policy 12.1.x/(TPD 7.0.2.0.0_86.28.0) to 12.3.x/(TPD 7.0.3.0.0_86.46.0)



Change Type	Change	MIB Module	Notification Name	Description	Status	OID
Added		TEKELEC-TPD-ALARMS-MIB	tpdCpuPowerLimitMismatch	The BIOS setting for CPU Power Limit is different than expected	CURRENT	1.3.6.1.4.1.323.5.3.18.3.1.3.41

NOTE: The Policy R12.2.x and R12.3.x use the same TPD version (7.0.3.0.0_86.46.0).