Oracle® Communications Policy and Charging Rules Function

PCRF Cable Network Impact Report/Feature Guide

Release 11.5

E61665-01

February 2015

ORACLE®

Oracle® Communications Policy and Charging Rules Function, Network Impact Report/Feature Guide, Release 11.5

Copyright © 2015 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, 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 on 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. 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.

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE/SCOPE

Purpose of this Feature Guide document is to highlight the changes in this release of the product that may have impact on the customer network, and should be considered by the customer during planning for this release.

1.2 DISCLAIMERS

This document summarizes Release 11.5.0.0 new and enhancement features, and the impacts of these features, at a high level. The Feature Descriptoins & Feature Requirements (FRS) documents remain the defining source for the expected behavior of these features.

2. REFERENCES

[1] Feature Description docs and Feature Specification docs
[2] Troubleshooting Guide Release 11.5 E55091 Revision 1.

2.1 ACRONYMS

AF	Application Function..
AM	PCMM Application Manager..
BOD BOD-AM	Bandwidth-on-Demand Application Manager
CLI	Command Line Interface
CMP	Configuration Management Platform. It implements basic OAM functionality for Oracle Communications Policy Management
CMTS	Cable Modem Termination System
DNS	Domain Name Server
ECN	Engineering Change Notice
EMS	Element Management System
GUI	Graphical User Interface
MA	Management Agent
MEAL	Measurements, Events, Alarms, & Logging
MGPI	Multiple Grants Per Interval
MPE	Multimedia Policy Engine
NE	Network Element
NMS	Network Mangement System
OSSI	Operation Support System Interface, XML base Interface between CMP and the EMS system for reporting statistical and KPI data
PCMM	Packet Cable MultiMedia
PCRF	Policy Control and Charging Rules Function
SNMP	Simple Network Management Protocol
TPD	ORACLE Platform Distribution
VIP	Virtual IP Address
XMI	External Management Interface
XSI	External Signaling Interface

3. OVERVIEW OF POLICY 11.5.0.0

This section provides an overview of the Policy11.5.0.0 release, as compared to the Policy 9.4 release.

3.1 ARCHITECTURE CHANGES

3.2 HARDWARE CHANGES

3.2.1 Hardware Supported & Backplane Interface details

Policy Release11.5 introduces support for the Sun Netra severs on Rack Mount Servers(RMS). The existing support for the HP G6 and Gen8 servers would be continued; which includes:

- HP ProLiant DL360G6
- HP ProLiant DL360G7
- HP ProLiant DL360pGen8
- HP ProLiant DL380pGen8
- Sun Netra X3-2 RMS

Note: The PP-5160 servers will not be supported in Release 11.5

Depending on the hardware type, the backplane interface may use a different NIC as shown in the following table

Hardware Type	OAM	Sig-A	Sig-B	Backplane
HP DL360 G6	Bond2=eth13	Bond1=eth11+eth12	Bond3=eth14	Bond0=eth01+eth02
HP DL360 G7	Bond2=eth13	Bond1=eth11+eth12	Bond3=eth14	Bond0=eth01+eth02
HP DL360pGen8	Bond0=eth01+eth11	Bond1=eth02+eth12	Bond2=eth03+eth13	Bond3=eth04+eth14
HP DL380pGen8	Bond0=eth01+eth11	Bond1=eth02+eth12	Bond2=eth03+eth13	Bond3=eth04+eth14
SUN Netra X3-2	Bond0.x=eth01+eth02	Bond1.y=eth03+eth04	Bond1.z=eth03+eth04	Bond3=eth13+eth14

3.2.2 Hardware Upgrade

No hardware upgrades are required with this release.

3.3 SOFTWARE CHANGES

3.3.1 Platform 6.7

Release 6.7 inherits all the functionality of Release 6.0.

Platform Component Versions

Component	Release
TPD	6.7
Comcol	6.3
PM&C	5.7
TVOE	2.7

3.4 UPGRADE OVERVIEW

This section provides an overview of the Upgrade activities for Policy Release 11.5.0.0.

3.4.1 Upgrade Path

For Policy: 9.4 → 11.5.0.0
For Policy: 9.3 → 11.5.0.0

3.4.2 Upgrade support

Upgrade is supported from Release 9.4 on all supported HP rack-mount server configurations (G6, G7, Gen8).

Source	Destination	Hardware	Direct-Link before upgrade	Direct-Link after upgrade
9.3	11.5/Cable	DL380G8	Disable	Enable
9.4	11.5/Cable	DL360G6	Enable	Enable
		DL360G7	Enable	Enable
		DL360G8	Enable	Enable
		DL380G8	Enable	Enable

3.4.3 Order of Upgrade

1) Firmware Upgrade --

The minimum firmware release required for Platform 6.7 is HP Solutions Firmware Upgrade Pack 2.2.5 (PN: 795-0000-316 and 795-0000-416). However, if a firmware upgrade is needed, the current GA release of the HP Solutions Firmware Upgrade Pack must be used.

2) Policy Upgrade in the following sequence –

CMP (Primary Site, then Geo-Redundant Site if present)

MA

MPE-R

MPE-S

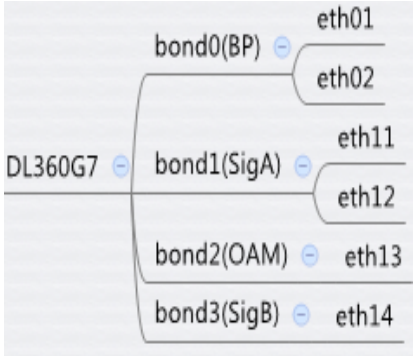
BoD-AM

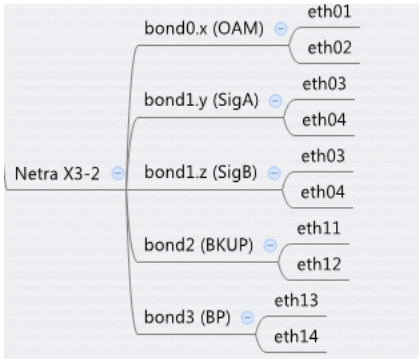
For Release 9.3 only CMP and MPE components can be upgraded since all 9.3 customers only have those 2 components implemented in their production system

3.5 POLICY REL. 9.3/9.4 TO REL. 11.5 MIGRATION/UPGRADE

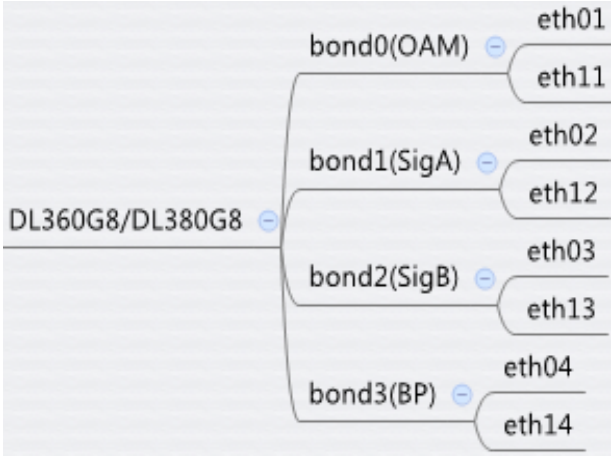
3.5.1 Upgrade Considerations

- The upgrade path from 9.4 to 11.5 requires that policy solution is on 9.4.1 release to be upgraded to 11.5, accordingly all 9.4 customers will need to upgrade to 9.4.1 if they are on earlier 9.4 revision before going to 11.5 release. Backplane details for all the supported hardware type for upgarde as follows;





- Back Plane link was not introduced in 9.3 Cable PCRF release, however it should be available and configured (cabled in the correct Ethernet ports “eth04 & eth14”) before upgrade since it is a mandatory setup to complete the upgrade process to 11.5 successfully.
- Upgrade shall be supported from Release 9.3 on only HP DL380 Gen8 servers, as these are the only servers deployed by customers running that release.



- The process of upgrading a Policy system from Release 9.3/9.4 to Release 11.5 takes a number of steps and may take a period of time that spans from several days to several weeks.
- During the migration period the PCRF system may have configuration where some of CMPs, MAs, MPEs, and BoD-AMs are running Release 9.3 or Release 9.4 software and some are running Release 11.5 software. This could result in some alarms which will be suppressed after the full solution is upgraded and reaches one coherent release. E.g. Alarms snapshot

MPE-R2 10.240.239.204	MPE	Minor	32509	10s / ---	Server NTP Daemon Not Synchronized	10/16/2014 13:40:02 EDT	
MPE-R2 10.240.239.204	MPE	Minor	32532	19s / ---	Server Upgrade Pending Accept/Reject	10/16/2014 13:39:53 EDT	
MPE-R2 10.240.239.204	MPE	Minor	70032	1m 15s / 10m 0s	QP direct link does not work as configuration	10/16/2014 13:38:57 EDT	
MPE-R2 10.240.239.204	MPE	Minor	78001	1m 3s / 1h 0s	Transfer of Policy jar files failed	10/16/2014 13:39:09 EDT	

- The Release 11.5 CMP would support 9.3 or 9.4 and 11.5 mixed-version configuration.
- The Release 11.5 CMP would be able to configure and monitor Release 9.3 or 9.4 configuration.

3.5.2 Release 9.3 Backplane Transition Requirements

- Release 9.3 systems with non-direct-link High Availability shall be tested pre-upgrade with direct-link backplane cables plugged in to the empty eth4 and eth14 interfaces.
- During the Release 9.3 to Release 11.5 upgrade process, the servers would be automatically reconfigured to use the direct-link backplane cables for High Availability data replication and cluster control functions (heartbeat, etc).
- The Release 9.3 to Release 11.5 upgrade process may automatically fail if the direct-link backplane cables are not plugged in correctly before initiating the upgrade process.

3.5.3 Accept Upgrade

- The primary purpose of Accept Upgrade operation is to clean up any files and data that are no longer needed from previous releases.
- This operation MUST be performed at some point before the 11.5 upgrade procedure is completed. This Operation Cleans up upgrade temp files, messages and RPMs etc.
- The “Accept Upgrade” operation will need to be executed for every cluster in the topology.
- After “Accept Upgrade” is executed, the server cannot be backed out to the previous release.

3.5.4 Release 11.5 Backout Support and Limitations

- Once CMP, MA, MPE, BoD servers are upgraded to Release 11.5, customer(s) may decide that a backout to the previous release is required. In that case, each individual server has to be backed out.
- If it is necessary to backout multiple servers, it is recommended that the systems be rolled back in the reverse order in which they were upgraded.
- Once all the servers in the system are backed out to the previous release, the servers in this PCRF system could be upgraded to another supported minor or major release. For example, if all of the servers in the PCRF system were backed out from Release 11.5-Build_A to Release 9.4 these servers could subsequently be upgraded to Release 11.5-Build_B
- Backout may be performed at any time after the upgrade, with the following limitations:
- if the “Accept Upgrade” operation has been performed, then backout to the previous release is no longer supported.
- If any new features have been enabled, they 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, that 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). The impact of any unexpected problem must be analyzed when it occurs to determine the best path forward (or backward) for the customer

4. CHANGES BY FEATURE (POLICY)

This section describes the changes introduced to the 11.5.0.0 product (as compared to the 9.4.x), organized by each feature separately.

4.1 EFFICIENT ADD/DELETE OF CLASSIFIERS IN RX-TRIGGERED MGPI UPDATE (PR 237633)

4.1.1 Description

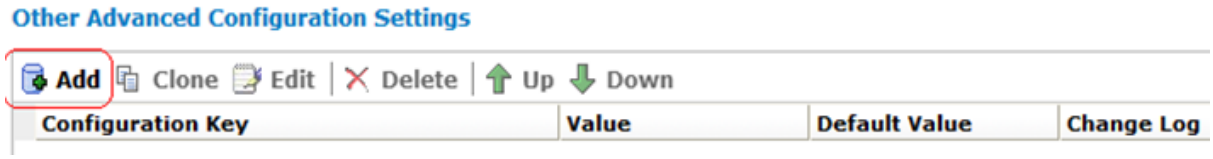
This is a customer-requested feature enhancement which will remove a practical limitation in current deployments. When MGPI functions are used with the MPE's Rx-to-PCMM functionality, services on high-line-count devices may be limited due to the possibility of hitting protocol maximum size limits. Exercising the PCMM option to send only added/deleted classifier information in a gate modification message, rather than re-expressing all current classifiers, will reduce the message size and avoid the maximum size issue.

- The behavior requires the use of Extended Classifier and/or IPv6 Classifier encoding – legacy Classifiers do not support the required attributes.
- The flag "DIAMETERPCMM.EnableEfficientMGPIClassifier"in Rcmgr can enable/disable this function. The flag DIAMETERPCMM.ExtClassifier" can control whether use extended classifiers for Rx-to-PCMM translation.
- Default values of both parameters are true after fresh Install/upgrade.

```
[root@yhu-mpe2 bin]# ./rcmgr
RcMgr> show cfg DIAMETERPCMM.ExtClassifier
  DIAMETERPCMM.ExtClassifier=true
RcMgr> show cfg DIAMETERPCMM.EnableEfficientMGPIClassifier
  DIAMETERPCMM.EnableEfficientMGPIClassifier=true
RcMgr>
```

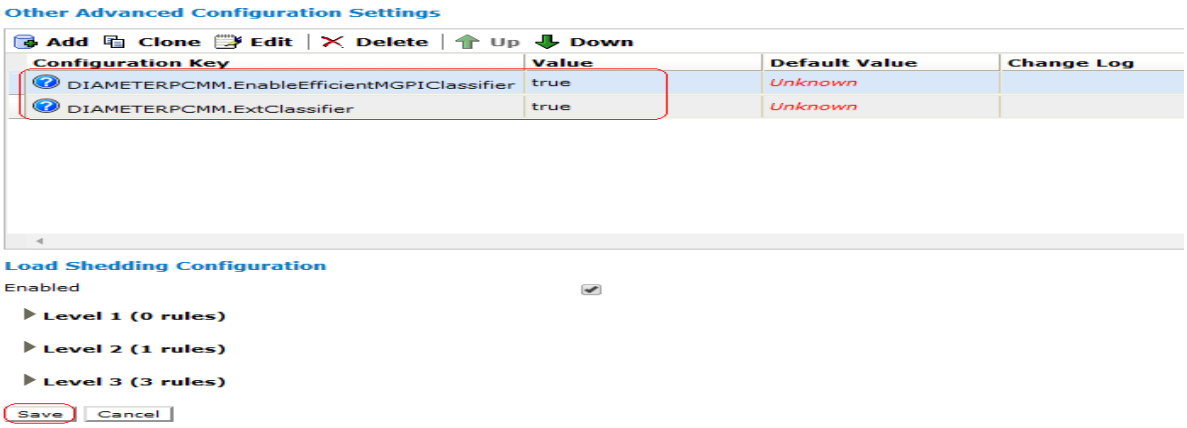
4.1.2 Manager GUI Form

- Enable/disable efficient MGPI classifier and extended classifier parameters can be set from CMP GUI also;
- Policy Server → Configuration → Policy Server tab of a configured MPE → Advanced → then "add " tab under "Other advanced configuration settings"

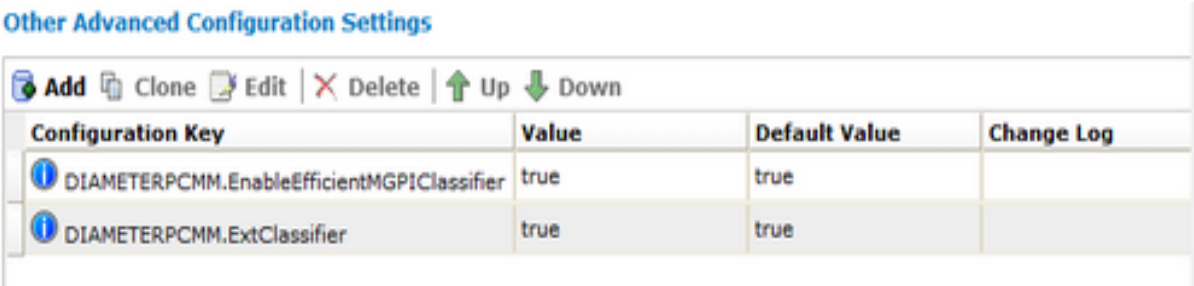


- Click Add , following window pops up;

- In Configuration Key field enter "*DIAMETERPCMM.ExtClassifier* " and in Value field enter "true".
- Similarly add another parameter using "*DIAMETERPCMM.EnableEfficientMGPIClassifier*" and "true" in Configuration Key and Value fields respectively then click "Save".
- Enable/disable efficient MGPI classifier and extended classifier parameters are entered in Advance configuration,



- Click Save tab to save the new parameters. New parameters are saved and displayed in the advanced window of the policy server



- **Add classifier to an existing MGPI gate**
  To add a new flow to MGPI gate, MPE translate Rx flow description to PCMM extended/IPv6 classifier, and set action to 0(Add classifier) and send the PCMM GateSet message only included this added classifier to CMTS. When the Action is set to 0 (Add classifier), the classifier will be added to the list of classifiers for the Gate
- **Update the classifier from an existing MGPI gate**
  To update a flow in existing MGPI gate, MPE translates Rx flow description to PCMM extended/IPv6 classifier, and set action to 1(Replace classifier). The ClassifierID will be set to the same with the classifier that will be updated. MPE will send the PCMM GateSet message only included this updated classifier to CMTS.

- **Remove classifier from an existing MGPI gate**
  To remove a flow from MGPI gate, MPE translates Rx flow description to PCMM extended/IPv6 classifier, and set action to 2(Delete classifier). The ClassifierID will be set to the same with the classifier that will be removed. MPE will send the PCMM GateSet message only included this removed classifier to CMTS

4.1.3 Dependency

None

4.2 CMTS/SUBNET ENHANCEMENTS-TRIGGER CMTS RE-DISCOVERY (SNMP) FROM OSSI COMMAND (PR 237630)

4.2.1 Description

Due to subnet re-allocation or operation/maintenance activity, customer may realize that the discovered subnet information for a CMTS is out of date, to automatically handle such situation an OSSI query/command will trigger subnet rediscovery for a specific CMTS.

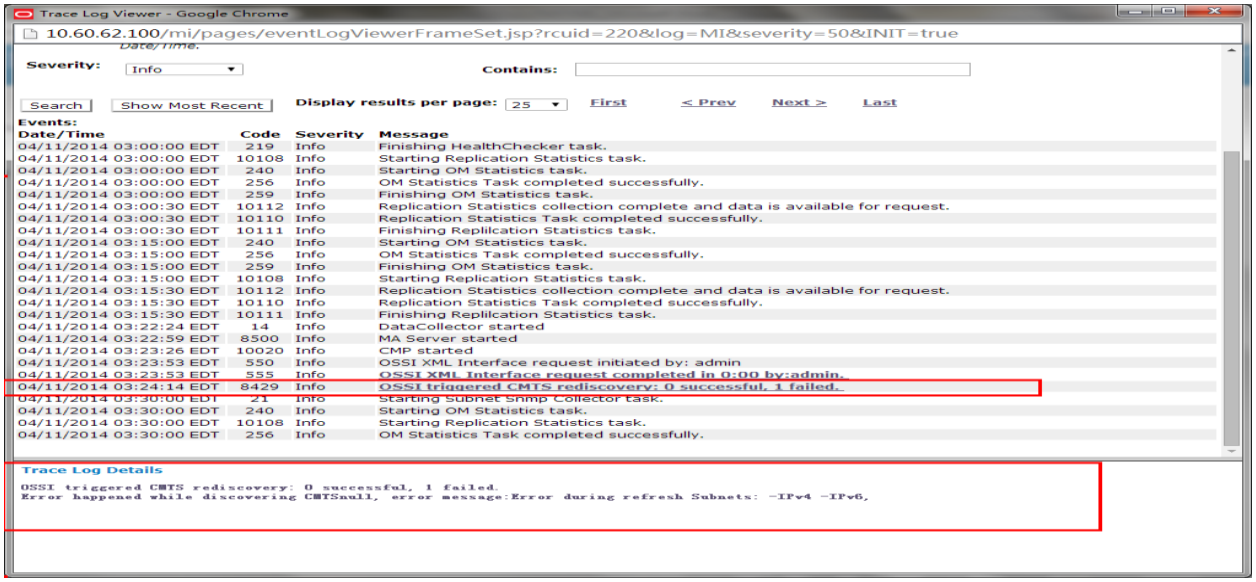
- To support OSSI trigger re-discovery CMTS subnet via SNMP, The new attributes 'Rediscovery' and 'DistributeImmediately' will be supported in **QueryNetworkElement**, **AddNetworkElement** and **UpdateNetworkElement** request.

- If Rediscovery attribute is special with 'yes', **AddNetworkElement** and **UpdateNetworkElement** request will also trigger CMP re-discovery after CMP create or modify CMTS successfully.

- The subnet rediscovery should support more than one existing CMTSs in one request, OSSI allows multiple<Name> elements in request XML. And response contains all discovered subnets.
- In one request, the number of <Name> elements are suggested not to exceed 100 when re-discovery trigger is enabled.
- While there are more than 100 <Name> elements in a quest, the system will not give back error. But it is possible to have a long time waiting for response. If the time out or exception happened while discovering some of the CMTSs, the response will return the error CMTSs with current subnets stored in MySQL database. Sample audit log below for reference.

2014-04-11 03:51:22	admin	10.60.4.106	Network Element - Discover	Discovered Network Element:
Failed to rediscover 1 CMTS(s). Error happened while discovering CMTS:[CMTS_public], error message:Error during refresh Subnets: -IPv4 -IPv6,				
2014-04-11 03:51:22	admin	10.60.4.106	Network Element - Modify	Network Element: CMTS_public (10.60.58.1) - Modified
2014-04-11 03:51:02	admin	10.60.4.106	Network Element - Batch Modify	Network Element batch modified
2014-04-11 03:51:02	admin	10.60.4.106	Network Element - Modify	Network Element: CMTS_public (10.60.58.1) - Modified

- The third-party EMS send OSSI request to re-discovery subnets on CMTS. CMP trigger MPE poll subnet information from CMTS via SNMP interface. CMP return back CMTS subnets information in OSSI response. Trace log snapshot below;



- This feature is active by default upon installation/Upgrade from pervious releases.

4.2.2 Dependency

None

4.3 CMTS/SUBNET ENHANCEMENTS-ENHANCE SUBNET-COLLECTION PERFORMANCE (PR 237635)

4.3.1 Description

In large Cable/DOCSIS network, even with the multiple MA servers for subnet discovery feature architecture, subnet collection task can run for several hours per execution cycle. This eventually limits the operator's ability to discover and distribute CMTS/Subnets info and ensure correct routing of policy/QoS requests. To reduce this time, refactoring or re-architecting the handling of SNMP queries are required.

- This feature is active by default upon installation/Upgrade from pervious releases.
- This enhancement includes to resolve the data inconsistency between CMP and MA while the network is down at the time when CMP is trying to fetch the CMTS' learned subnets from MA.
- The basic enhancement is to change the original serial process for retrieving CMTS data on MA to be in a concurrent manner. The subnets data from CMTS will be retrieved using the multi-thread mechanism
- The multi-thread value is set by this parameter **CollectorTask.maxthreadpoo**l in dc. properties file , the default value is 5
- Subnet SNMP collector task is listed in scheduled task

4.3.2 Dependency

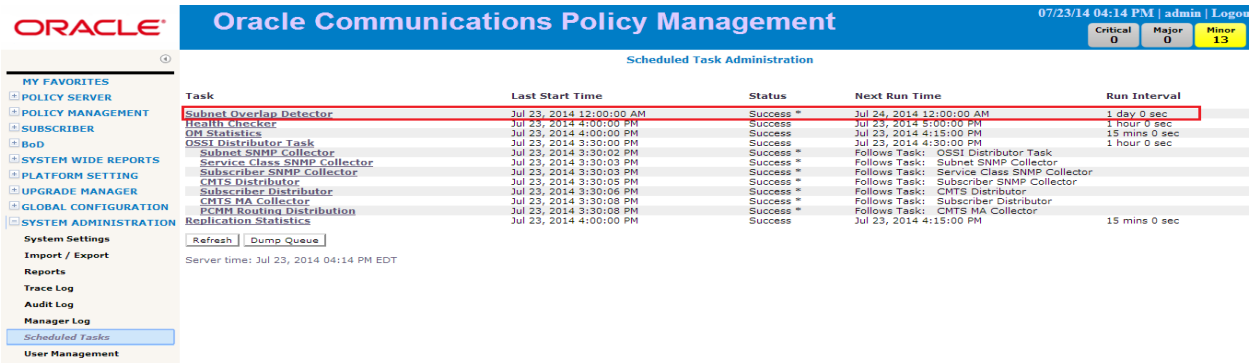
None

4.4 CMTS/SUBNET ENHANCEMENTS-DETECT THE DUPLICATE/OVERLAPPING SUBNETS ON DIFFERENT CMTSS (PR 237632)

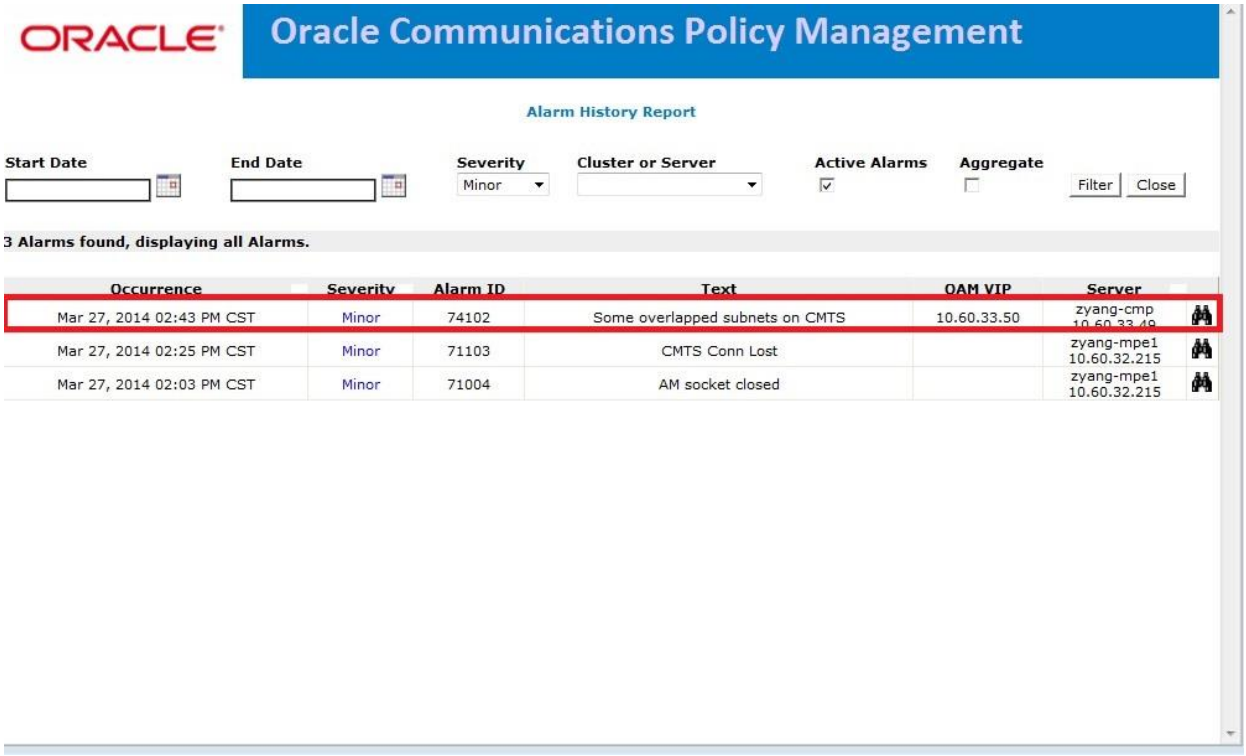
4.4.1 Description

The Policy Management solution interacts with Cable DOCSIS networks with very large scale and operational complexity, and dependent on accurate subnet-topology data (which may be provisioned or discovered, or a combination of both) in order to correctly route incoming requests to downstream policy servers and CMTSs. Large deployments include thousands of CMTSs connecting hundreds of thousands of IPv4 subnets, and IPv6 prefix counts are increasing rapidly and may surpass IPv4 due to Prefix Delegation techniques. Especially where automated subnet topology discovery is used in large networks, duplicate and overlapping subnet routes can occur due to discovery timing, network maintenance, or other conditions including user error. Customers have expressed a desire for the Policy Management solution to provide a notification when duplicate or overlapping subnets are associated with different CMTSs.

- This feature implements the function to detect the duplicate or overlapping subnets on different CMTSs. In the current system, subnets in CMTS are configured on CMP. The same subnet can be configured in different CMTSs without any inspection. So there is a potential risk that duplicate or overlapping subnets are configured on different CMTSs when subnets are increasing rapidly. These duplicate or overlapping subnets can cause not only the failed session but also poor performance .So we need a task to detect the duplicate or overlapping subnets.
- The new task's name is "Subnet Overlapping Detector", it will collect all the subnets on CMTSs and notify the administrator of duplicate subnets. These duplicate or overlapping subnets will be recorded in trace logs and dc logs.
- The task is enabled by default. It will start at twelve o 'clock every night. Subnet Overlap Detector task is active & scheduled by default after fresh installation/upgrade



- There is the alarm to inform users that there are duplicate or overlapping subnets on CMTSs. The alarm ID is 74102. The description of the alarm is “Some overlapped subnets on CMTS”. This alarm will be cleaned by itself when the task runs next time. If duplicate or overlapping subnets exist, the task will alarm again. The Severity is Minor. We can see the alarm information like this:



4.4.2 Dependency

None

4.4.3 Limitations

Since this task will collect all the subnets into memory, there is the potential risk that causes OOM. The suggestion is that the task runs when the system is free. The requirement specifies there are 10,500 CMTS in CMP and each CMTS with 350 subnets. We can roughly estimate the total consumption of the memory. It nearly needs to consume 470M of memory. In our physical machine, the DC java heap size is 6G. So this task should not bring great influence to memory.

4.5 BOD ENHANCEMENTS- MULTI-CLASSIFIERS SUPPORTED IN A PCMMSERVICE (PR 237631)

4.5.1 Description

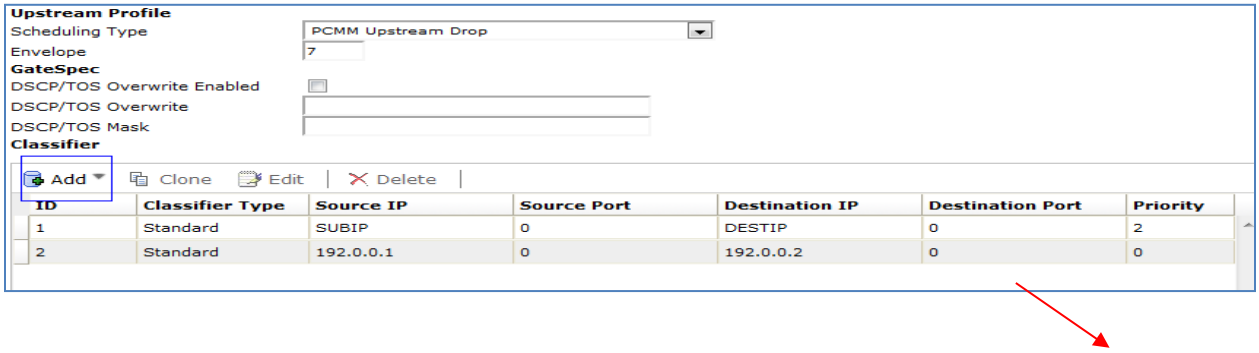
A recent CableLabs ECN (ECN-MM-N-13.0697-10) for the PCMM (PKT-SP-MM-I06-110629) specification clarifies the possibility to include both IPv4 Extended Classifiers and IPv6 Classfiers in the same GateSet message.

In 9.3/9.4 version, a PCMMService only has one type of Classifier which means that only a pair of standard/extended/ipv6 Classifiers (upstream&downstream) can be created. A recent update in PCMM specifications to include both IPv4 Extended Classifiers and IPv6 Classifiers in the same GateSet message.

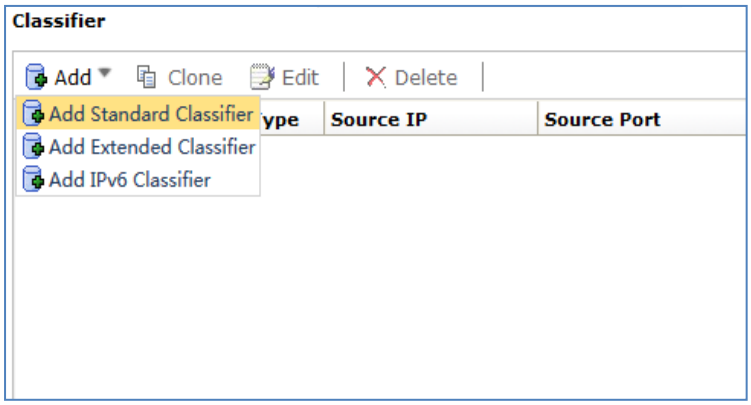
This feature allow users to create(or modify) the PCMMService that contains multi Classifiers at the same time. In 11.5 release, a PCMMService can contain multi Classifiers which means that user can create session with multiple standard /extended/ipv6 Classifiers ,only extended/ipv6 types can be mixed.

4.5.2 Manager GUI Form

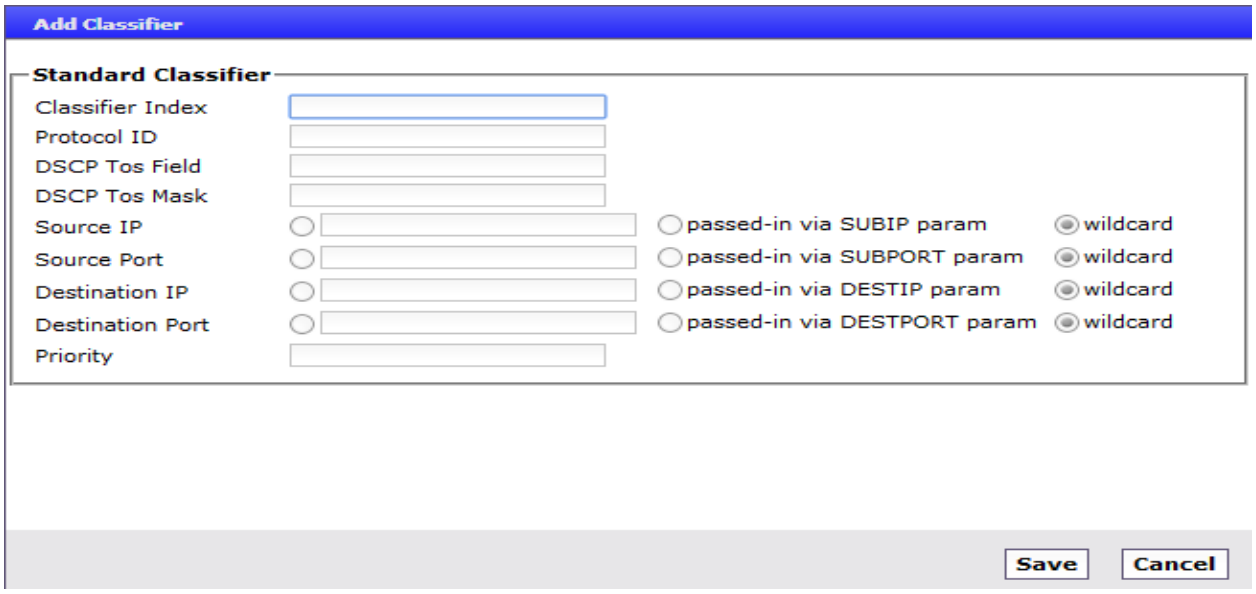
This feature is supported by default after fresh installation of a new Cable System or upgrade from previous releases. An add button is provided in CMP GUI under BoD->Services->Modify-> to add classifier.



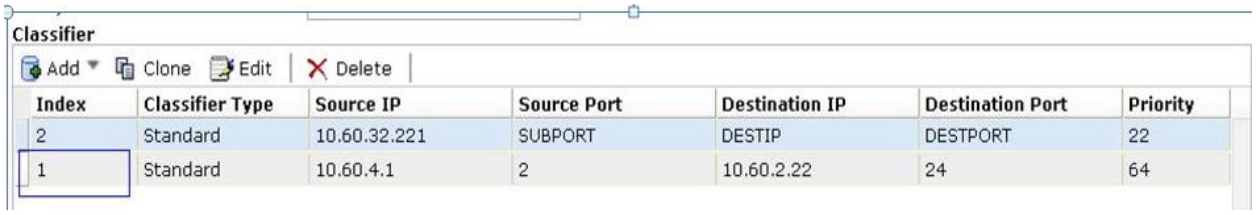
- Click Add button a drop down menu appears with standard menu.



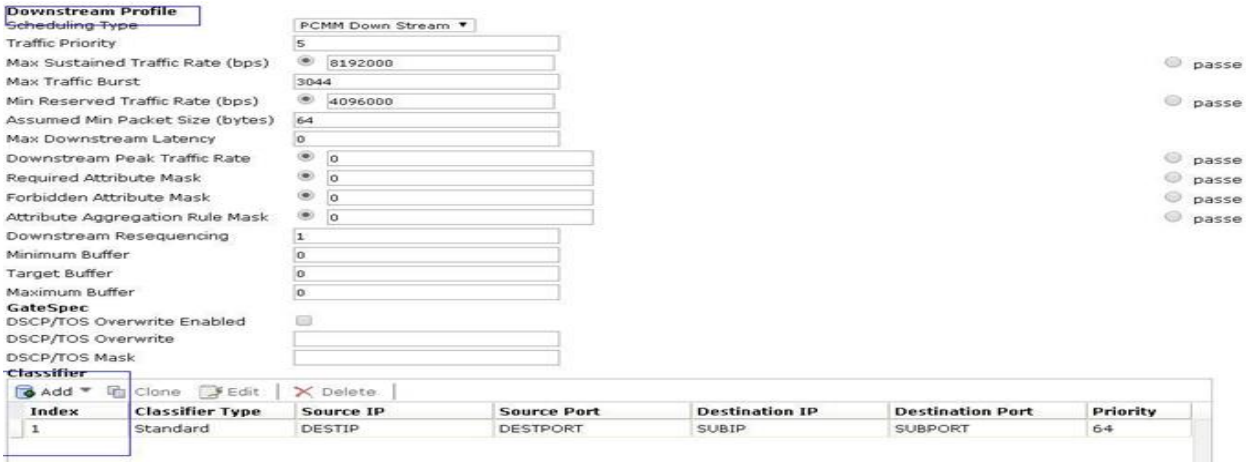
- Multiple Classifiers' parameters can be configured in the CMP as shown in below Figure. Parameters have a little difference between Standard Classifier and other type Classifiers.



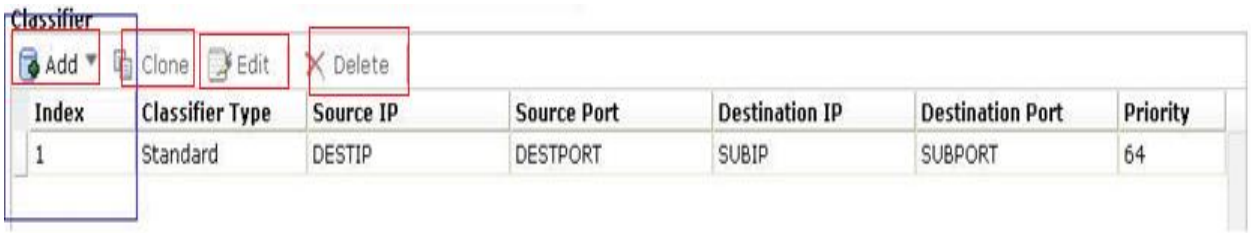
- Classifiers in upstream and downstream profile can be associated by classifier Index. And upstream and downstream classifier can be matched by classifier Index.



Index	Classifier Type	Source IP	Source Port	Destination IP	Destination Port	Priority
2	Standard	10.60.32.221	SUBPORT	DESTIP	DESTPORT	22
1	Standard	10.60.4.1	2	10.60.2.22	24	64



- There are also “Copy”, “Edit”, “Delete” buttons on the page of viewing detail pcmm service. The buttons are used to clone/modify/remove the detail service.



4.5.3 Dependency

None

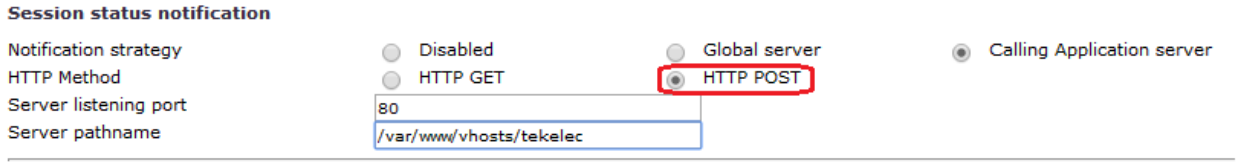
4.6 BOD ENHANCEMENTS-BOD ASYNCHRONOUS NOTIFICATION WITH GET OR POST (PR 237639) & MULTIPLE DESTINATION IP ADDRESSES FOR BOD NOTIFICATIONS (PR 237650)

4.6.1 Description

In Release 9.4 BoD only uses HTTP GET method to send notifications. This feature enables BoD to choose the HTTP method depending on the configurations on CMP when send notification to notification servers.

BoD supports both IPV4 and IPV6 IP addresses. Content of the notifications will be recorded in the trace log in DEBUG level after notifications are sent successfully. This feature is active by default upon installation/Upgrade from pervious releases.

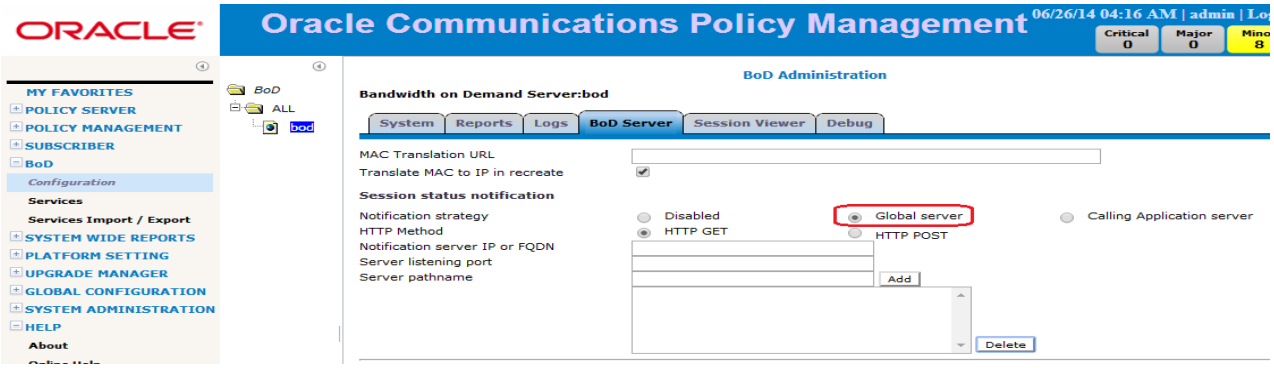
GET or POST selection page of CMP GUI under BoD-> Configuration-> select the Configured BoD from the navigation tree, click tab BoD Server-> Modify-> select Calling Application Server and then select the desired method for notification GET or POST and then Save;



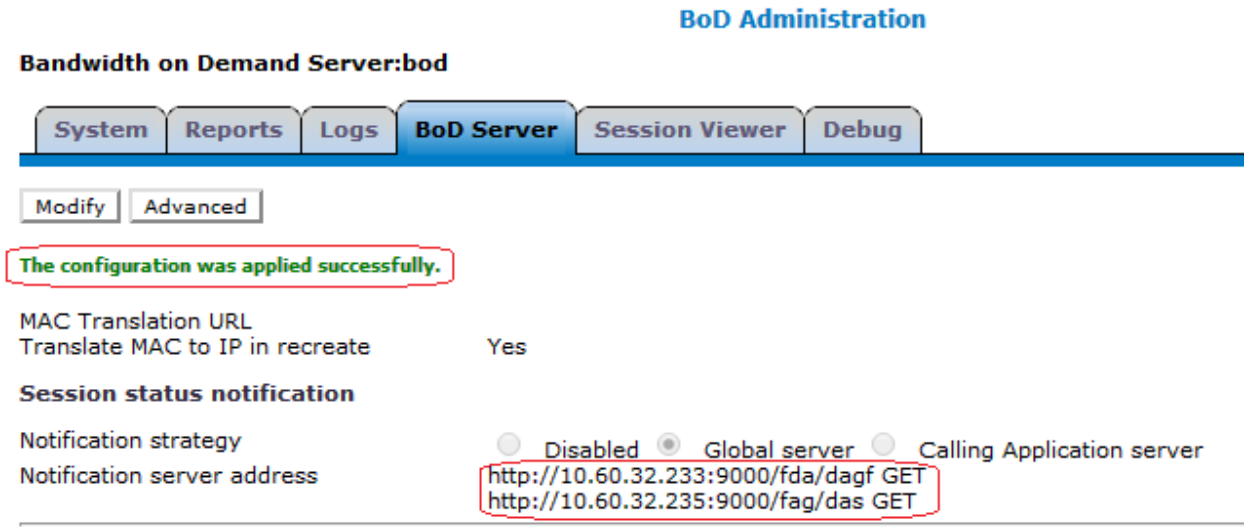
When multiple notification destinations are configured, BoD will send notifications to all of the configured destinations.

4.6.2 Manager GUI Form

CMP configuration support each notification destination is defined with an independent IP address, destination port and server path and HTTP method. Multiple destination configuration page given below; CMP GUI under BoD-> Configuration-> select the Configured BoD from the navigation tree, click tab BoD Server-> Modify-> Choose "Global server" as the notification strategy: Fill in the notification server IP or FQDN, port and the path name then hit add for each notification destination server to be configured then Save:



A confirmation message should appear in CMP GUI that configuration was successfully set and the configured notification servers' details displayed in BOD server's session status notification section:



4.6.3 Dependency

None

4.6.4 Limitations

If there's configuration change in the processing of sending notification out, we may lost several (very tiny) notifications. This is caused by we have shutdown HttpClient to reconfigure. To alleviate the issue, we'll re-configure HttpClient when network connection related configurations are changed.

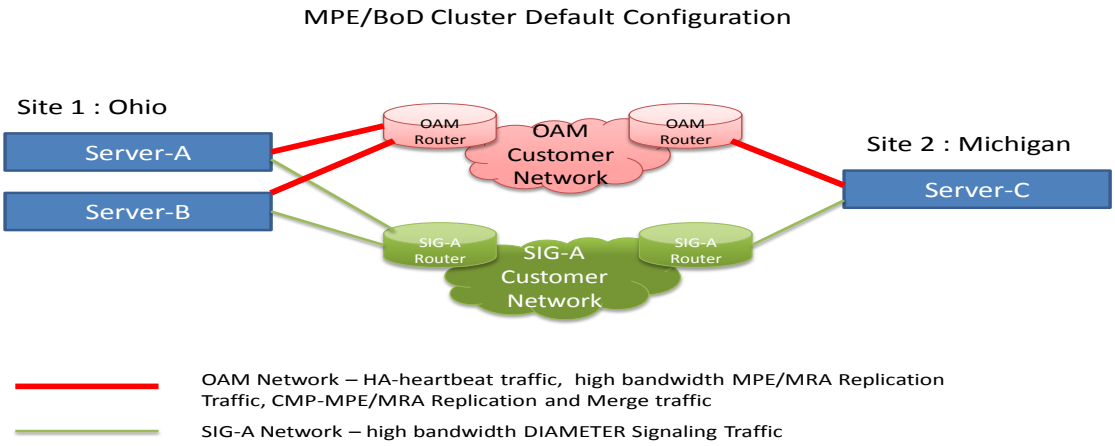
When fail-over happens, the un-sent notifications will be all lost.

4.7 REDUNDANCY ENHANCEMENT - MPE AND BOD GEO-REDUNDANCY REPLICATION VIA NON OAM NETWORK (PR 237638)

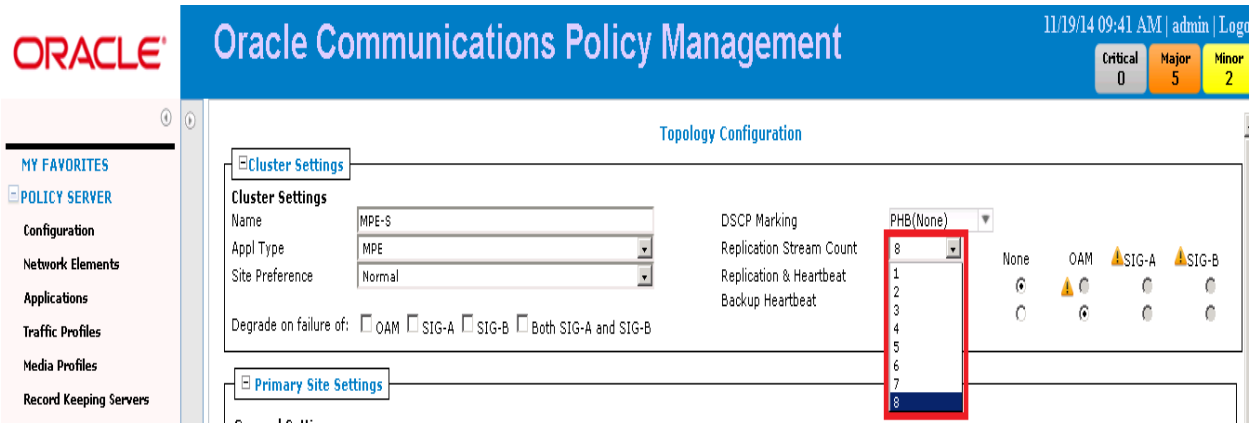
4.7.1 Description

In previous releases, by default the OAM network carries all replication traffic for site to site Geo Redundancy and for some of the Operators, it is not ideal to use OAM network for such traffic, this feature gives operators the option who can choose to send the MPE/BoD replication traffic on the SIG-A, SIG-B or OAM network.

This feature is active by default after fresh installation of a new Cable System or upgrade from previous releases. And by default OAM network carries all replication traffic to support previous configurations behavior.

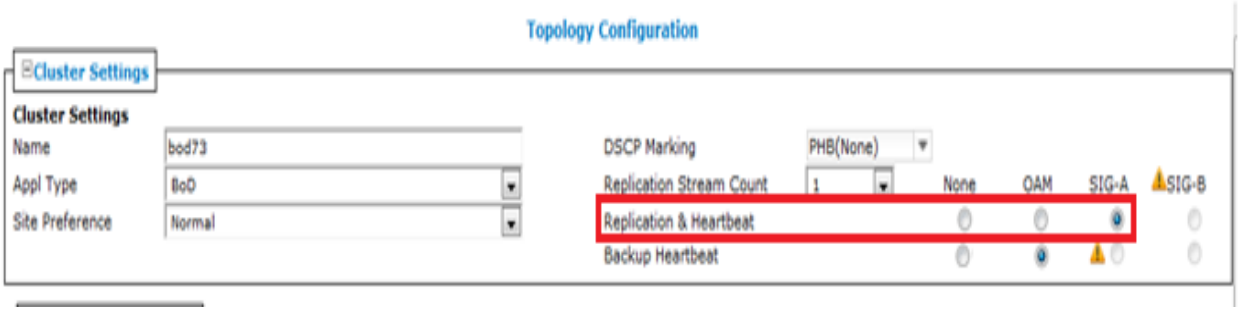


- **Multi-Stream WAN Replication:** Customer may configure additional socket connections to improve inter-site MPE/BoD Replication. Replication Stream Count supports one (1) to eight (8) stream for replications. The values to use for configuration Replication Stream Count are driven by the customer's choices.
- The WAN Streams settings shall only be used if a Spare server is configured in secondary site.



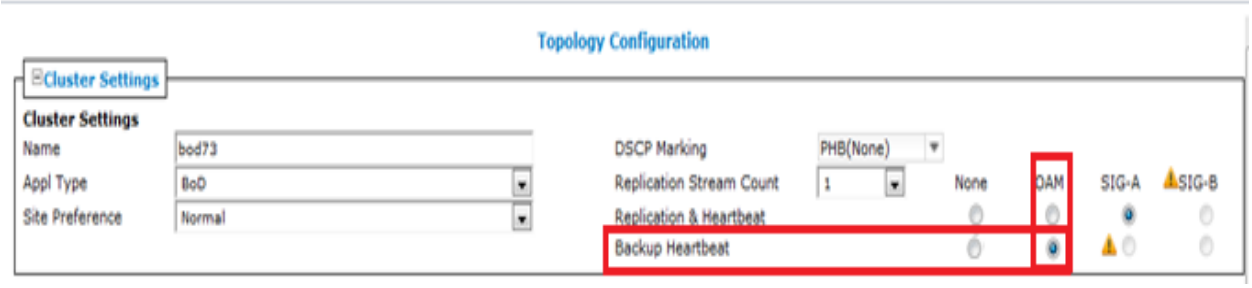
- **Separate MPE/BoD Replication Traffic onto specific VLAN:**

  MPE/BoD Replication from Server-A/B to Server-C may be put on a non-OAM network such as SIG-A or SIG-B. In below snapshot SIG-A network is used for MPE/BoD Replication & HA HB Network and the OAM network is configured as the secondary HA HB network.



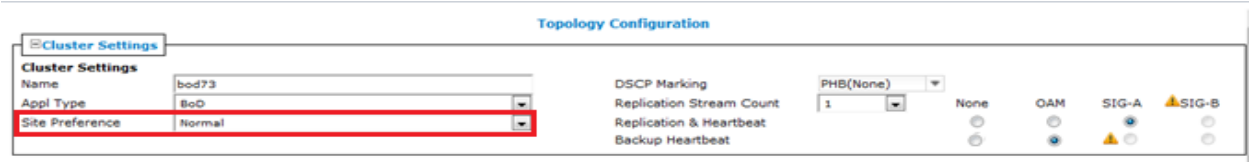
- To separate replication traffic onto SigA/B network, The SigA or SigB static IP is needed config individually in Server A/B/C's Path Configuration
- This configuration has no impact on HA/local replication between servers in primary site.

- **Separate Secondary HA Heartbeat Traffic onto specific VLAN:** Secondary HA Heartbeat Traffic from Server-A/B to Server-C may be put on a specific network such as OAM, SIG-A or SIG-B. OAM network could be configured as the secondary HA HB network if SIG-A network is used for MPE/BoD Replication & HA HB Network.



- If the primary HA HB network experiences failure, and the customer has configured a secondary HA heartbeat path, that path is used to send heartbeats between Server-A/B and Server-C. The use of the secondary path helps prevent split brain in some failure cases.

- **Dual Active Resolution**:
- In Platform 5.2, when the two sites lose contact the servers at both sites go active which is known as dual-active or split-brain.
- Dual-active resolution feature in Platform 6.7 improves the robustness of resolving a split-brain condition with MPE/BOD using PCRF-GR feature.
- This feature makes Active resolution predictable. The Active server at the preferred site shall maintain the active role after split brain is healed. The Active server at the non-preferred site shall demote itself to a non-Active server (Standby or Spare).



- The feature described above prevent both Active servers from demoting to Standby after Split brain is healed.

4.7.2 Dependency

None

4.8 REDUNDANCY ENHANCEMENT- CAUSE A FAILOVER IF BOTH LINKS IN A SIG-A OR SIG-B BOND ARE DOWN. (PR 237640)

4.8.1 Description

- The OAM and Signaling Interfaces in Policy products on rack-mount hardware make use of two separate Ethernet ports with an OS-level bonded configuration. Previous TPD-based software releases have not monitored the OAM and Signaling interfaces for failures at the logical level (e.g. caused by doubly disconnected cables), perhaps since this constitutes a double-failure case for the solution(single failures being accommodated by the bonded link pairs).
- Similarly, past TPD-based releases did not degrade a server's status or cause an HA or GR fail-over based on the loss of both physical interfaces in a logical SIG interface (perhaps due to above reasons, and/or ambiguity in the roles and criticality of OAM, SIG-A and SIG-B interfaces if both are configured)
- Policy components operating on rack-mount servers support a configurable option to demote a server on which a complete logical Signaling Interface (e.g. SIG-A or SIG-B) is detected to have failed.
- User can configure HA status failure of each cluster according to network connection on OAM, SIGA, SIGB, SIGA AND SIGB or some combinations
- User can configure HA status failure of each cluster according to network connection on OAM, SIGA, SIGB, SIGA AND SIGB or some combinations in this scope. The relationship between each options is "OR". It means HA status on active server would be failure when network connection of one network interface option in the combination is down. The valid network interface option in this combination should be running with virtual cluster IP address.

OAM	SIGA	SIGB	SIGA AND SIGB	Logical Expression
√	o	o	√	OAM || (SIGA AND SIGB)
√	√	×	×	OAM || SIGA
×	√	×	×	SIGA
√ - select × - not select ○ – select or not select (It means in this case, the result should be same regardless this				

- The SIG-A and/or SIG-B interfaces is not considered to have failed, unless a virtual IP address is actually configured on that interface. This ensures that an un-configured interface will not cause a fail-over or component outage
- This feature is active by default after fresh installation of a new Cable System or upgrade from previous releases. The default behavior is compatible with previous TPD releases.

CMP GUI base configuration would allow user to decide which network interface combination which would degrade server HA status.

4.8.2 Dependency

None

4.9 OPTIMIZE THE CMP PERFORMANCE BY USING LAZY LOADING (PR 237799)

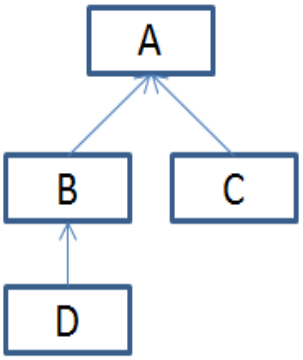
4.9.1 Description

In previous release, in most cases, CMP would load initial data and all of its dependent data that it might be never used. This might cause to take long time to load program. This feature would use lazy loading to benefit the performance of data access. It is an extension of existing approach with deep fetch.

This feature allows a developer enable lazy loading on an object that should defer loading until the point at which it is needed. This meaning is that lazy loading objects are only loaded as they are specifically requested.

This is a sample to show the data loading process. Assume that there is an object A, and object B & C associated with A, object D associated with B. The diagram as figure 1:

As CMP deep fetch mode, if loading object A, object B, C and D is also loaded at the same time, regardless of these dependency object is used or not.



- If object B enable lazy loading, then loading object A, only Object C would be loaded. Object B would defer loading until it need.
- If object D enable lazy loading, then loading object A, Object B & C would be loaded. Object D would defer loading until it need.
- If object B enable lazy loading, then loading object A, only Object C would be loaded. Object B would defer loading until it need.
- If object D enable lazy loading, then loading object A, Object B & C would be loaded. Object D would defer loading until it need.
- The operator would login system much faster, because it might save from loading network elements and subnets that it never intend to use at this process.
- It might take less time when associating network element with policy server, because some data consistency checking is not need to involve network elements and subnets.
- The data of KPI dashboard might be displayed much faster, because it might save from loading network elements and subnets that it never intend to use at this process.

4.9.2 Dependency

None

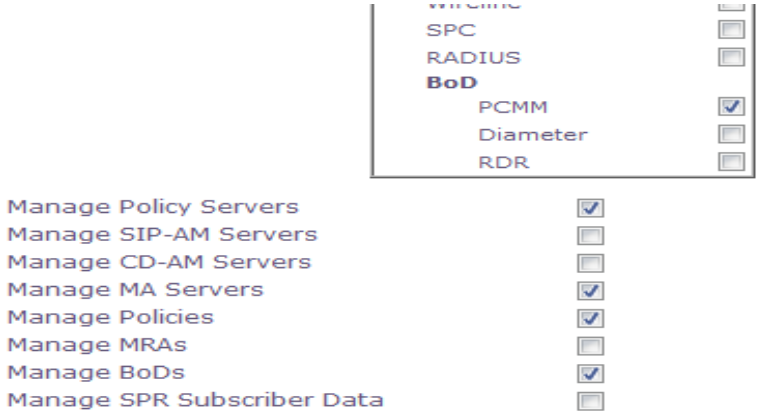
4.10 REFINE THE STAT ID (PR 238096)

4.10.1 Description

In Cable 9.4, we have 8 BoD server statistic's ID conflict with 11.5 wireless statistics from 93 to 100. To avoid error occurs in 11.5 CMP mix mode server when upgrade from 9.4, CMP need add special work in Mi-Agent and Data Collector.

Because these BoD statistics does not support OSSI in 9.4, OM Statistic DC task will ignore Stats data with ID range from 93 to 100. In Cable mode, Data Collector in CMP will not collect any statistics with conflict Stats ID from MPE if BoD server is configured. No impact on MPE Cable statistics.

When 9.4 Legacy CMP has BoDs features mode selected before upgrade, CMP will display Stats with ID 93 to 100 as BoD statistics data correlation. CMP will prevent Data Collector from collecting Stats data with ID 93 to 100 from MPE if none of wireless mode is selected



- After change in 11.5, BoD statistics will use new ID range from 120 to 150 which has no conflict with wireless statistics.
- 9.4 BoD Statistics IDs which is conflict with 11.5 wireless Statistics.

11.5 (Wireless)	9.4 (Cable)
TYPE_DYNAMIC_QUOTA = 93;	TYPE_BOD_PCMM = 93
TYPE_RETURNED_1 = 94;	TYPE_BOD_DIAMETER = 94
TYPE_RETURNED_2 = 95;	TYPE_BOD_HTTP = 95
TYPE_PDN_RAT_TYPE = 96;	TYPE_BOD_SOAP = 96
TYPE_DIAMETER_SY = 97;	TYPE_BOD_GATEREPORT = 97
TYPE_DIAMETER_SY_ADAPTOR = 98;	TYPE_BOD_RDR = 98
TYPE_AF_RAT_TYPE = 99;	TYPE_BOD_PCMM_ADMISSION = 99
TYPE_COMCOL = 100;	TYPE_BOD_DIAMETER_ADMISSION = 100

- Stats ID range from 120 to 150 are reserved for BoD statistics future use.

11.5 (Cable) BoD Statistics IDs after adjust:

```
TYPE_BOD_PCMM              = 120;
TYPE_BOD_DIAMETER          = 121;
TYPE_BOD_HTTP              = 122;
TYPE_BOD_SOAP              = 123;

TYPE_BOD_GATEREPORT        = 124;
TYPE_BOD_RDR               = 125;
TYPE_BOD_PCMM_ADMISSION    = 126;
TYPE_BOD_DIAMETER_ADMISSION = 127;
```

4.10.2 Dependency

None

4.11 PLATFORM CFG NEED ADD MENU TO CONFIG MODE(WIRELESS, CABLE) (PR 238090)

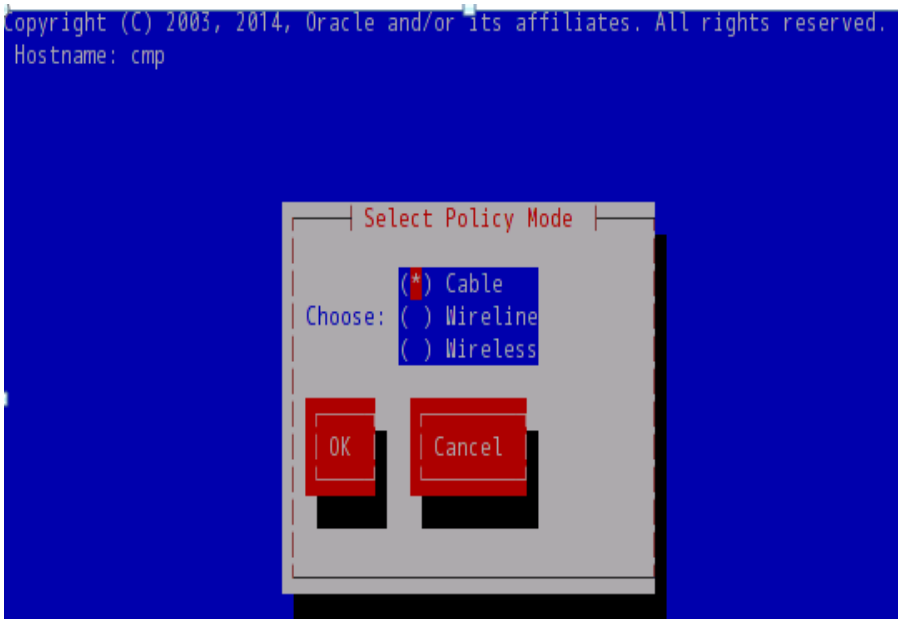
4.11.1 Description

Oracle requires Policy team integrates all products into one GA release; the GA release can be used for different markets and different customers. But there are many different requirements and features from different markets, some of these requirements may be conflict with others. It is impossible to enable all features without any impact in one GA release. QP software must enable some features and disable other features according to user's decision.

During the process of Policy product fresh installation/upgrade, the script "qpFeature --add" should be called with parameters from component RPMs which contain features for different market/customer. After installation, user must select one of modes from PLATCFG menu before performing any operations. Menu "Perform Initial Configuration" would not be permitted before there is known running mode.

4.11.2 Platcfg GUI

To Change/Correct the Policy Mode go to platcfg-->Policy Configuration-->Set Policy mode, Select the desired mode and click save



- The running mode would be same as the GA release it upgrade from.
- The different features register to MODE should be enable/disable according to configure MODE.

4.11.3 Dependency

None

4.12 SUPPORT ETHERNET AUTONEG PARAMETERS AND BOND PRIMARY_RESELECT (BUG 19108332)

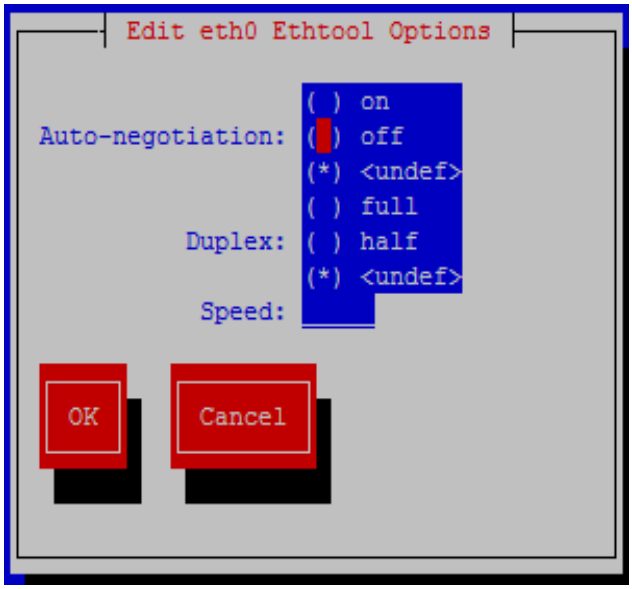
4.12.1 Description

In TPD 6.7, netAdm supports –autoneg/--speed/--duplex options. This makes it possible to set Ethernet speed and duplex parameters.

If none of these options are specified, auto-negotiation is assumed.

4.12.2 Platcfg GUI

In the platcfg GUI, under "Network Configuration" → "Network Interfaces" → "Edit Interface", choose an interface, it pops out a dialog asking "Would you like to configure Ethernet Options?", if you answer "Yes", then a dialog appears to allow you specify the speed/duplex options:



4.12.3 Dependency

None

4.13 SET RESTRICTIVE DAEMON UMASK AND USER UMASK (PR 221797)

4.13.1 Description

This feature sets the umask setting to 0027 so that the permissions on any new file (unless otherwise specified) are:

For the same user: readable and writable

For the users in the same group: read-only

For other accounts: not accessible.

Note: This setting only applies to newly created files. If the files existed before the system is upgraded to release 11.5, their modes are not changed.

This feature also sets daemon processes provided by COMCOL and all daemon processes provided by policy products to 0027 for umask.

It also sets users with a UID of less than 5000 to have a umask of 0027; users with a UID equal or greater than 5000 have the umask set to 0077.

4.13.2 Dependency

None

4.14 SUPPORT CUSTOMER-CUSTOMIZABLE DEFAULT PASSWORDS (PR 232877)

4.14.1 Description

- The feature adds the support of customizable passwords for system accounts.
- TPD 6.7 supports customizable passwords for system accounts.
- TPD 6.7 does not provide any GUI for changing passwords. System commands like "passwd" can be used to change passwords.
- In following cases Policy products use "root" ssh login.

-- In platcfg, "Policy Configuration" --> "Cluster File Sync", some configuration files in /etc/camiant are copied to the mates in the cluster. And some scripts are executed over ssh.

-- In the script rsyncUtil.pl, is used by tomcat and data collector to synchronize some data in a cluster. And rsync uses ssh as transportation channel.

-- The upgrade manager uses ssh to communicate with target servers.

- All these use cases require ssh keys are properly exchanged. After SSH keys are exchanged, changing root password should not affect the functionalities.

4.14.2 Dependency

None

4.15 ROOT SSH LOGIN ONLY ALLOWED WHEN KEYS ARE EXCHANGED (PR 239591 & 240246)

4.15.1 Description

PR 239591: Disable password-based root ssh login. Root ssh login is allowed only when keys are exchanged.

PR 240246: Create a new utility to exchange root SSH keys.

- Prior Release 11.5, policySSHKey.pl and platcfg menu “Exchange SSH keys” are used to provision SSH keys among servers in topology. But all of them depend on hard-coded root password. This means these utility and function need remote password-based root SSH login to exchange keys between servers in the Policy topology.
- In Release 11.5, password-based root SSH login will be disabled. A tool rootSshPass is created to enable/disable password-based root SSH login. When the system is installed or upgraded to release 11.5, command “rootSshPass --revoke” is executed automatically.
- After rootSshPass --revoke command, the root login is revoked through ssh with password. You can still login from console. You can still login after exchanging public SSH keys.

4.15.2 Dependency

None

4.16 ALARM FOR TIME ZONE CHANGE (PR 234708)

4.16.1 Description

- In policy release 11.5, we should support and detect change in timezone done from platcfg.
- When the user edits time zone in platcfg "Service Configuration" → "Timezone" → "Edit", and select a timezone other than the current set one, an alarm 70050 will be triggered.
- All policy components need to be restarted in order to use the new timezone settings. The alarm 70050 is cleared when qp_procmgr is restarted.

4.16.2 Dependency

None

4.17 PRODUCT REBRANDING (PR 234735, 235040)

4.17.1 Description

In user interface of policy 11.5, all visible occurrences of “camiant” should be replaced to “oracle” or “policy server”; all visible occurrences of “tekelec” should be changed to “oracle”. In TPD 6.7, the copyright notice already changes “tekelec” to “oracle”.

The top level menu entry in platcfg for QP utilities was named “Camiant Configuration”, it should be changed to “Policy Configuration”.

File names and folder names are not changed in release 11.5. Some files and folders will still have “camiant” in the names:

/etc/camiant

/opt/camiant

/var/camiant

/opt/TKLCcomcol/camiant

/opt/plat/etc/BackupTK/camiant*.xml

/opt/plat/etc/savelogs_plat.d/camiant*

Database names also do not change in release 11.5. There will still be database “camiant” and “camiantdc” in mysql. There will also be database “camiant” in comcol Imysql.

.

4.17.2 Dependency

None

5. POLICY OAM CHANGE SUMMARY

5.1.1 Alarms Delta

Event Id	Name and Description	Delta
31131	**DB Ousted Throttle Behind–** DB ousted throttle may be affecting processes.	New Event Added
31236	**HA Link Down–** High availability TCP link is down.	New Event Added
31285	**HA Split Brain Recovery Entry–** High availability split brain recovery entered	New Event Added
31286	**HA Split Brain Recovery Plan–** High availability split brain recovery plan	New Event Added
31287	**HA Split Brain Recovery Complete–** High availability split brain recovery complete	New Event Added
32345	**Server Upgrade snapshot(s) invalid–** This alarm indicates that upgrade snapshot(s) are invalid and backout is no longer possible..	New Event Added
32346	**OEM hardware management service reports an error–** This alarm indicates that OEM hardware management service reports an error.	New Event Added
32347	**The hwmgmtcliStatus daemon needs intervention–** This alarm indicates the hwmgmtcliStatus daemon is not running or is not responding.believed to be correct on start-up. Recovery will often will require rebooting the server.	New Event Added
32536	**Server Upgrade Snapshot(s) warning–** This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon otherwise snapshots will become 100% full and invalid.	New Event Added

70005	**QP Cluster Status–** One or more servers in the cluster are not at QP Blade Status -- The QP Blade Status is not available for one or more servers in the cluster.	New Event Added
70029	**QP Peer Node Bonded Interface is Down–** Indicates QP peer node bonded interface is down.	New Event Added
70030	**QP Backplane Bonded Interface is Down–** Indicates Backplane bonded interface bond3 is down.	New Event Added
70031	**QP degrade because one or more interfaces are down–** QP degrade because one or more interfaces are down	New Event Added
70032	**QP direct link does not work as configuration–** QP degrade because one or more interfaces are down	New Event Added
70050	**QP Timezone Change Detected–** Timezone has been changed using platcfg. Application needs to be restarted	New Event Added
71103	**PCMM CONN LOST–** PCMM Conn Lost -- The connection was lost to the specified CMTS or downstream policy server.	New Event Added
74605	**SUBSCRIBER TRACE BACKUP FAILURE–** The script responsible for backing up the subscriber trace log has failed.	New Event Added
75109	**The Mediation Server has achieved 80% of the maximum number of users in SPR. –** Achieve 80% maximum number of users in SPR.	Alarm heding has changed from [Achieve 80% maximum number of users in SPR] to [The Mediation Server has achieved 80% of the maximum number of users in SPR]

79105	**MEDIATION_SOAP_TOO_BUSY –** Mediation Server SOAP provisioning interface reaches busy state; load shedding begins.	New Event Added
79106	**SPR_CONNECTION_FAILED –** Created connection to SPR failed.	New Event Added
79107	**MEDIATION_DISK_QUOTA_EXCEED –** Sync directory disk quota exceeded.	New Event Added
79108	**MEDIATION_DISK_NO_SPACE –** No space left on device.	New Event Added
79109	**SPR_LICENSE_LIMIT–** Achieve 80% maximum number of users in SPR.	New Event Added