Oracle® Communications

Diameter Signaling Router

PCA Feature Activation Guide

Release 8.5

F33372-01

October 2020

ORACLE®

Oracle Communications Diameter Signaling Router PCA Feature Activation Procedure, Release 8.5.

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

My Oracle Support (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.

See more information on My Oracle Support (MOS).

Table of Contents

List of Tables

List of Figures

List of Procedures

1. Introduction

1.1 Purpose and Scope

This document defines the procedures to activate the Policy and Charging Application (PCA) feature on a DSR network element (NE). This procedure may be run either 1) as part of a new DSR installation, after the standard DSR installation is complete, but before the NE is in service, or 2) on an in-service DSR NE, where the PCA feature is activated during a planned maintenance window to minimize the impact to network traffic.

This document also provides a procedure to deactivate PCA after it has been activated. Refer to Section 3 for a discussion of deactivation.

Configuration of PCA following successful activation is beyond the scope of this document. Please refer to the PCA User's Guide for guidance on PCA configuration post activation.

No additional software installation is required before executing this procedure. The standard DSR installation procedure has loaded all of the required software, even if the PCA feature is activated at a later time.

1.2 References

[1] DSR Software Installation and Configuration Procedure 2/2

[2] DSR Policy Charging Application User's Guide

[3] DSR PDRA Configuration Work Instruction, WI006808

[4] DSR PDRA Activation/Deactivation Work Instruction, WI006835

[5] DSR PCA Activation and Configuration

[6] DSR GLA Feature Activation Procedure

[7] DSR Software Upgrade Guide

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
DA-MP	Diameter Agent Message Processor
DB	Database
DPI	Diameter Plug-In
DSR	Diameter Signaling Router
GLA	Gateway Location Application
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IP	Internet Protocol
IPFE	Internet Protocol Front End
MP	Message Processing or Message Processor

Acronym	Definition
NE	Network Element
NO	Network OAM
NOAM	Network OAM
PDRA	Policy DIAMETER Routing Agent
SBR	Session Binding Repository (when used without the "B" or "S" suffix, refers to both binding and session SBRs)
PCA	Policy and Charging Application
PCRF	Policy and Charging Rules Function
OAM	Operations, Administration and Maintenance
SSH	Secure Shell
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface
SBR-B	Session Binding Repository – Binding
SBR-S	Session Binding Repository – Session
SOAM	System OAM

1.4 Terminology

Table 2. Terminology

Term	Definition
Communication Agent	Software infrastructure that allows applications to communicate with the SBR databases in a reliable manner.
ComAgent	Same as Communication Agent
NOAM	Network Operations and Maintenance
SBR-B	Holds network-wide subscriber binding information. Maps subscriber keys to the PCRF that hosts the subscriber's policy rules.
SBR-S	Holds session information used for routing in-session messages.
SOAM	System Operations and Maintenance

1.5 General Procedure Step Format

Where it is necessary to identify the server explicitly on which a particular step is to be taken, the server name is given in the title box for the step (e.g., “ServerX” in Figure 1. Example of a Procedure Step).

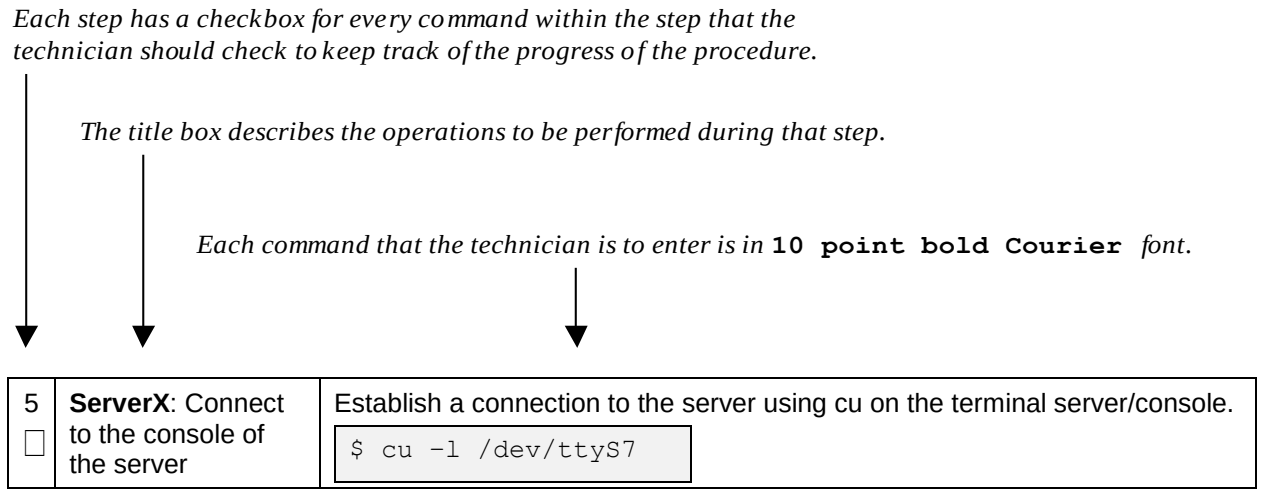


Figure 1. Example of a Procedure Step

1.6 Release Document Matrix

Table 3. PCA Activation\Configuration Procedure Reference Table

DSR Release	Reference
DSR 5.1/6.0	[3] and [4]
DSR 7.0	[1] and [2]
DSR 7.1/7.2	[1] and [5]
DSR 7.3/7.4	[7]
DSR 8.x	[1], [2], and [6]

2. Feature Activation Overview

This section lists the required materials and information needed to execute the feature activation. In addition, Table 4. *Pre-Feature Activation Overview* through Table 9. *Post-Feature Deactivation Overview* provide estimates of the time required to execute the procedures. These tables can be used to estimate the total time necessary to complete the feature activation. The timing values shown are estimates only – use these tables to plan the timing of the activation, **not** to execute the procedure. The detailed procedure steps to be executed begin in Section 5.

2.1 Definition of Activation for the PCA Feature

The precise meaning of activation varies from feature to feature. This section briefly defines what activation means with respect to the PCA feature.

The main components of a PCA system include the PCA (DSR) application, the binding database (hosted by the Session Binding Repository, i.e., SBR), and finally the ComAgent which provides a interface and means to enable the PCA MPs and the SBR MPs communicating to each other via reliable ComAgent routing services. Subscriber data concerning binding and session information is populated in the SBR-B and SBR-S respectively by the Policy Diameter Routing Agent (Policy DRA).

PDRA/PCA DSR application requires configuration of SBR-Binding as well as SBR-Session servers and ComAgent connections to these SBR servers.

All software required to run GLA is available by default as part of a DSR release installation or upgrade. GLA cannot be activated until after PCA is activated. The process of activating the feature simply makes proper use of software elements and file system files already present to change the behavior of the DSR NE.

Before PCA feature activation, there are no PCA menu items visible on the SOAM GUI and NOAM GUI and there is no PCA-related processing taking place on the DA-MP(s).

After feature activation, all selectable PCA menu items are present on the SOAM GUI and NOAM GUI, allowing full PCA configuration and provisioning. Specifically, for PCA application, the top-level PCA folder is visible on the Main Menu, and a new entry is added to the **Diameter - >Maintenance -> Applications** table, showing PCA and its state. Activation of PCA does not affect DSR signaling behavior except for process restarts necessary during the activation.

After activation:

DSR setup is ready to act as PCA application subject to the PCA configuration.

Important: Upon PCA feature activation, it is not automatically enabled. Activation simply means the mechanism for configuring PCA behavior is in place. But the DA-MP(s) acts on PCA provisioning information only after PCA has been enabled (via the **Diameter -> Maintenance -> Applications** screen). PCA should not be enabled until after the appropriate provisioning data has been entered. PCA provisioning is beyond the scope of this document, refer [2] for PCA configuration. Furthermore, for proper operation of PCA, Communication Agent and PCA application assumes the Remote servers IP addresses corresponding to the ComAgent HA service (for Binding Resource) are routable/reachable. However, these networking setup/concerns are beyond the scope of the activation procedure. After PCA activation, please refer [2] for PCA configuration.

2.2 Feature Activation Overview

2.2.1 Pre-Feature Activation Overview

The pre-activation procedures shown in the following table may be executed outside a maintenance window if desired. Procedure completion times shown here are estimates. Times may vary due to differences in database size, network configuration and loading, user experience, and user preparation.

Table 4. Pre-Feature Activation Overview

Procedure	Elapsed Time (Hours:Minutes)		Feature Activation Preparation Procedures
	This Step	Cum.	
System Topology Check (0)	0:00-1:00	0:00-1:00	• Verify Network Element Configuration data. • Verify Server Group Configuration data. • Analyze and plan DA-MP restart sequence.
Perform Health Check (0)	0:01-0:20	1:01-1:20	• Verify server status. • Log all current alarms.

2.2.2 Feature Activation Execution Overview

The procedures shown in the following table are executed inside a single maintenance window.

Either procedure 4 or procedure 5 should be executed as per the requirement. Procedure 4 should be executed when NOAM and SOAM servers for at least one DSR site are installed and configured. Procedure 5 must be repeated if one or more DSR sites are added to a DSR network and PCA is to be used on the new sites.

Procedure completion times shown here are estimates. Times may vary due to differences in database size, network configuration and loading, user experience, and user preparation.

Table 5. Feature Activation Execution Overview

Procedure	Elapsed Time (Hours:Minutes)		Feature Activation Execution Procedures
	This Step	Cum.	
Perform Health Check (0)	0:01-0:05	0:01-0:05	• Verify all servers in the network are on the same DSR release. • Verify proper PCA feature state. • Verify server status. • Verify server and server group configurations. • Log all current alarms.

Procedure	Elapsed Time (Hours:Minutes)		Feature Activation Execution Procedures
	This Step	Cum.	
Feature Activation for Entire Network (0) or Feature Activation for Newly Added Sites (0 or Feature Activation on Active NOAM (0) or Feature Activation on Standby NOAM (0) or Feature Activation on Active SOAM (0) or Feature Activation on Standby SOAM (0)	0:10-0:40	0:11-0:45	• Log out of NOAM/SOAM GUI. • SSH to active NOAM. • Login as the **admusr**. • Change directory to /usr/TKLC/dsr/prod/maint/loaders/activate. • Execute the feature activation script. • Log into NOAM or SOAM GUI. • Verify the Policy and Charging folder. • Verify Maintenance screen. • Log into NOAM GUI (Optional). • Restart each active DA-MP server. • Verify Maintenance screen.
Restart Process (0)			• Restart process on DA-MP servers. • Restart process on SBR servers.

2.2.3 Post-Feature Activation Overview

The procedures shown in the following table can be executed outside a maintenance window. Procedure completion times shown here are estimates. Times may vary due to differences in database size, network configuration and loading, user experience, and user preparation.

Table 6. Post-Feature Activation Overview

Procedure	Elapsed Time (Hours:Minutes)		Feature Activation Completion Procedures
	This Step	Cum.	
Perform Health Check (0)	0:01-0:05	0:01-0:05	• Establish GUI session on the NOAM VIP. • Verify the KPIs. • Verify the Measurements. • Verify GUI left hand menu item.
Perform Health Check (0)	0:01-0:05	0:02-0:10	• Establish GUI session on the SOAM VIP. • Verify GUI left hand menu item.

3. Feature Deactivation Overview

3.1 Pre-Feature Deactivation Overview

The procedures shown in the following table can be executed outside a maintenance window. Deactivation procedure times are only estimates as the reason to execute a deactivation has a direct impact on any additional deactivation preparation that must be done. Times may vary due to differences in database size, network configuration and loading, user experience, and user preparation.

Table 7. Pre-Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Pre-Feature Deactivation Procedures
	This Step	Cum.	
Perform Health Check (0)	0:01- 0:05	0:01-0:05	• Establish GUI session on the SOAM VIP. • Verify GUI left hand menu item. • Establish GUI session on the NOAM VIP. • Verify server status. • Log current alarms.
Verify PCA application state and deactivate GLA (0)	00:01-00:05	0:02-0:10	• Establish GUI session on the SOAM VIP. • Verify PCA record in **Diameter -> Maintenance -> Applications**. • Verify GLA record in **Diameter -> Maintenance -> Applications**. • Deactivate GLA, if activated.
Unconfigure PCA Functions (PDRA and OCDRA) (0)	00:10-00:40	0:12-0:50	• Establish GUI session on the NOAM VIP. • Unconfigure PDRA function. • Unconfigure OCDRA function.
Disable Diameter Connections (0)	00:01-00:05	0:13-0:55	• Establish GUI session on the SOAM VIP. • Disable PCA-specific diameter connection.
Disable application (0)	00:01-00:05	0:14-1:00	• Establish GUI session on the SOAM VIP. • Disable PCA application.
Remove DSR configuration data (0)	00:01-00:05	0:15-1:05	• Establish GUI session on the SOAM VIP. • Remove PCA-specific DSR configuration.
Remove Resource Domain configuration data (0)	00:01-00:05	0:16-1:10	• Establish GUI session on the NOAM VIP. • Remove PCA-specific resource domain configuration.
Remove Place Associations configuration data (0)	00:01-00:05	0:17-1:15	• Establish GUI session on the NOAM VIP. • Remove Place Association configuration.
Remove Place configuration data (0)	00:01-00:05	0:18-1:20	• Establish GUI session on the NOAM VIP. • Remove Place configuration.

3.2 Feature Deactivation Execution Overview

Deactivation procedure times are only estimating as the reason to execute a deactivation has a direct impact on any additional deactivation preparation that must be done. Times may vary due to differences in database size, network configuration and loading, user experience, and user preparation.

Table 8. Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Feature Deactivation Procedures
	This Step	Cum.	
Feature Activation for Entire network (0) or Feature Deactivation on single site (0)	0:01 – 0:40	0:01 – 0:40	• Log out of active NOAM/SOAM GUI. • SSH into active NOAM. • Login as the **admusr**. • Change directory to /usr/TKLC/dsr/prod/maint/loaders/deactivate • Execute the feature deactivation script. • Log into NOAM or SOAM GUI • Verify the Policy and Charging folder. • Log into NOAM GUI • Restart each active DA-MP server. • Verify Maintenance screen.

3.3 Post-Feature Deactivation Overview

The procedures shown in the following table are executed inside a maintenance window. Deactivation procedure times are only estimates as the reason to execute a deactivation has a direct impact on any additional deactivation preparation that must be done. Times may vary due to differences in database size, network configuration and loading, user experience, and user preparation.

Table 9. Post-Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Post Feature Deactivation Procedures
	This Step	Cum.	
Move SBR Servers to OOS State (0)	0:01-0:05	0:01-0:05	• Establish GUI session on the NOAM VIP • Move SBR server to OOS
Remove SBR Servers from Server Groups (0)	0:01-0:05	0:02-0:10	• Establish GUI session on the NOAM VIP • Remove SBR server from server group
Reboot the Servers (0)	0:10-1:00	0:12-1:05	• Identify the sequence of the server to be rebooted • Reboot the server in sequence

Procedure	Elapsed Time (Hours:Minutes)		Post Feature Deactivation Procedures
	This Step	Cum.	
Perform Health 0, 0, and 0)	0:01-0:05	0:01-0:20	• Verify server status. • Log all current alarms. • Verify the KPIs. • Verify the Measurements. • Verify GUI menu does not shows PCA sub-menu

4. Feature Activation Preparation

This section provides detailed procedures to prepare a system for PCA feature activation. These procedures are executed outside a maintenance window.

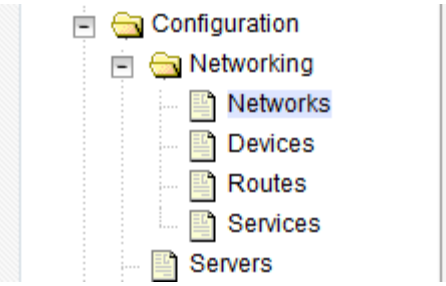
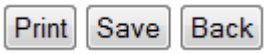
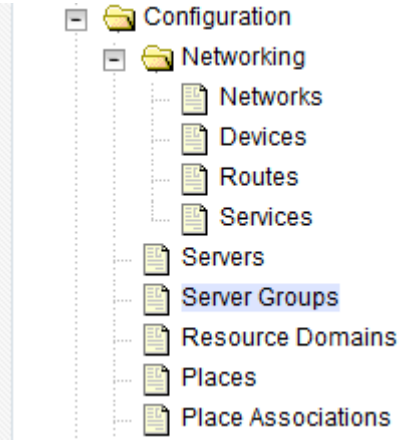
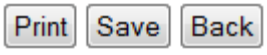
4.1 System Topology Check

This procedure is part of feature activation preparation and is used to verify the system topology of the DSR network and servers.

System Topology Check

S T E P #	This procedure verifies system topology. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

System Topology Check

2. ☐	**NOAM VIP GUI**: Verify network configuration data	Navigate to **Configuration -> Networking -> Networks**.  Click **Report**.  Verify the configuration data is correct for your network. **Save** or **Print** this report to keep copies for future reference. 
3. ☐	**NOAM VIP GUI**: Verify server configuration	Navigate to **Configuration -> Server Groups**.  Click **Report**.  Verify the configuration data is correct for your network. **Save** or **Print** this report to keep copies for future reference. 

System Topology Check

4. ☐	Analyze and plan DA-MP restart sequence	During PCA Activation procedure 6 for activation of PCA on an existing system, it will be necessary to restart the application process on each DA-MP server. This step is to plan the order and level of parallelism for the process restarts such that signaling disruption is minimized. Analyze system topology and plan for any DA-MPs which will be out-of-service during the feature activation sequence. Analyze system topology gathered in Steps 2 and 3. Determine exact sequence which DA-MP servers will be restarted (with the expected out-of-service periods). ***Note***: It is recommended that no more than 50% of the MPs be restarted at once.

4.2 Perform Health Check

This procedure is part of feature activation preparation. This may be executed multiple times but must also be executed at least once within the time frame of 24-36 hours before the start of the maintenance window in which the feature activation will take place.

Perform Health Check (Feature Activation Preparation)

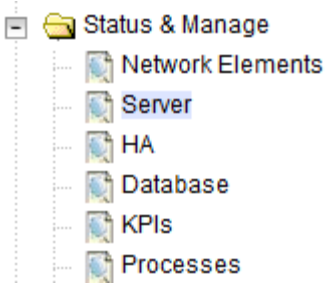
S T E P #	
	This procedure provides steps to perform needed health checks. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
1. ☐	**NOAM VIP GUI**: Login

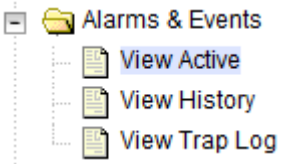
Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of:

```
http://<Primary_NOAM_VIP_IP_Address>
```

Login as the **guiadmin** user:

Perform Health Check (Feature Activation Preparation)

<table>
<tr>
<td>2. ☐</td>
<td>NOAM VIP GUI: Verify server status</td>
<td>Navigate to Status & Manage -> Server.
 

Verify all Server Status is Normal (Norm) for:
Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table>
Do not proceed to feature activation if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.
If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the feature activation. If there are Major or Critical alarms present, these alarms should be analyzed before proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms. Contact My Oracle Support (MOS) for assistance as necessary.</td>
</tr>
<tr>
<td>3. ☐</td>
<td>NOAM VIP GUI: Log current alarms</td>
<td>Navigate to Alarms & Events -> View Active.
 

Click Report.
 

Save or Print this report to keep copies for future reference.
 
</td>
</tr>
</table>

5. Feature Activation

Before feature activation, perform the system health check in Section 4.2. This check ensures the system is ready for feature activation. Performing the system health check determines which alarms are present in the system and if feature activation can proceed with alarms.

******* WARNING *******

If there are servers in the system, which are not in Normal state, these servers should be brought to the Normal or the Application Disabled state before the feature activation process is started.

If alarms are present on the server, contact My Oracle Support (MOS) to diagnose those alarms and determine whether they need to be addressed or if it is safe to proceed with the feature activation.

Please read the following notes on feature activation procedures:

- Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:
  - Session banner information such as time and date.
  - System-specific configuration information such as hardware locations, IP addresses, and hostnames.
  - ANY information marked with “XXXX” or “YYYY” where appropriate, instructions are provided to determine what output should be expected in place of “XXXX or YYYY”
  - Aesthetic differences unrelated to functionality such as browser attributes: window size, colors, toolbars, and button layouts.
- After completing each step and at each point where data is recorded from the screen, the technician performing the feature activation must initial each step. A check box should be provided. For procedures which are executed multiple times, the check box can be skipped, but the technician must initial each iteration the step is executed. The space on either side of the step number can be used (margin on left side or column on right side).
- Captured data is required for future support reference.

5.1 Pre-Activation Procedures

5.1.1 Perform Health Check

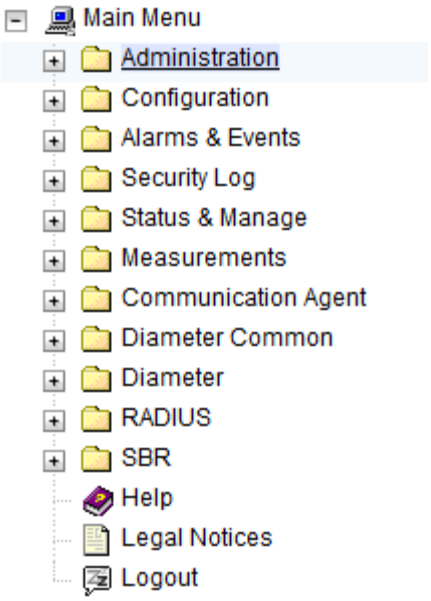
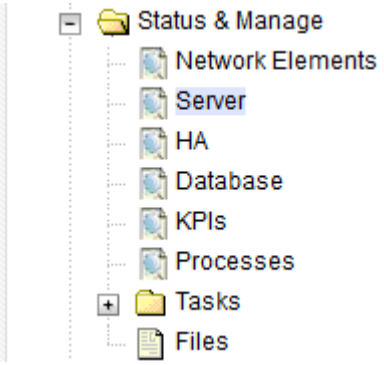
This procedure is used to determine the health and status of the network and servers. This must be executed at the start of every maintenance window.

Note: The Health Check procedure below is the same as the Health Check procedure described in Section 4.2 when preparing for feature activation, but it is repeated here to emphasize that it is being re-executed if Section 4.2 was performed outside the maintenance window.

Perform Health Check (Pre Feature Activation)

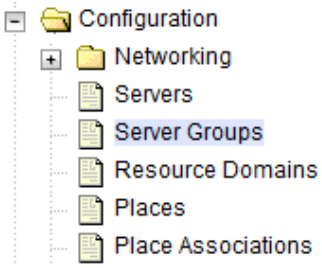
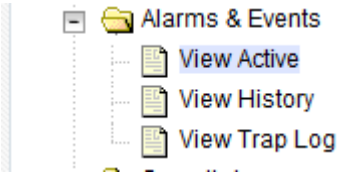
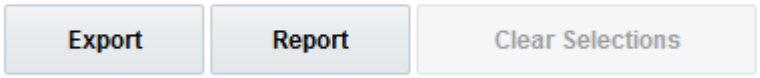
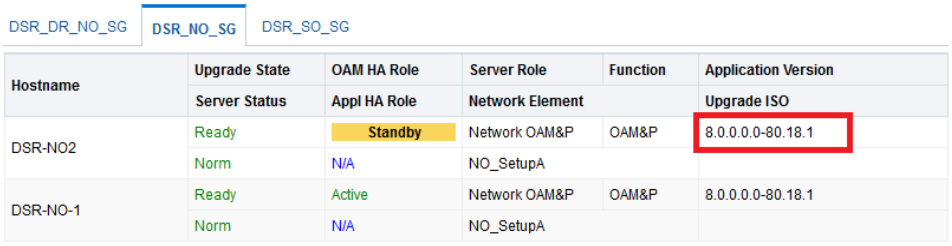
S T E P #	This procedure performs needed health checks. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

Perform Health Check (Pre Feature Activation)

<table>
<tr>
<td>2. ☐</td>
<td>NOAM VIP GUI: Verify PCA Folder is not Present</td>
<td>Under Main Menu, verify the Policy and Charging folder is NOT present.
 
</td>
</tr>
<tr>
<td>3. ☐</td>
<td>NOAM VIP GUI: Verify server status</td>
<td>Navigate to Status & Manage -> Server.
 

Verify all Server Status is Normal (Norm) for:
Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc).
<table>
<tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
<tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr>
</table>
Do not proceed to feature activation if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.
If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the feature activation. If there are Major or Critical alarms present, these alarms should be analyzed before proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms. Contact My Oracle Support (MOS) for assistance as necessary.</td>
</tr>
</table>

Perform Health Check (Pre Feature Activation)

4. ☐	**NOAM VIP GUI**: Verify server configuration	Navigate to **Configuration -> Server Groups**.  Verify the configuration data is correct for your network.
5. ☐	**NOAM VIP GUI**: Log current alarms	Navigate to **Alarms & Events -> View Active**.  Click **Report**.  **Save** or **Print** this report to keep copies for future reference. 
6. ☐	**NOAM VIP GUI**: Check the software version on all servers	Navigate to **Administration -> Software Management -> Upgrade**. Verify the Upgrade ISO column shows the correct release number for all servers in the DSR network. ***Note***: All servers in the network must be on the same DSR release when activating PCA. 

Perform Health Check (Pre Feature Activation)

7. ☐	**NOAM VIP GUI**: Check the Upgrade Acceptance status on all servers.	Navigate to **Administration -> Software Management -> Upgrade**. Verify the Upgrade State column does not show **ACCEPT** or **REJECT**. ***Note***: Upgrade must be accepted on all servers before activating PCA. DSR_DR_NO_SG | DSR_NO_SG | DSR_SO_SG Upgrade State should be **Ready**. If the Upgrade State is **ACCEPT OR REJECT**, follow the Installation Guide [1] or Upgrade Guide [7] (whichever applies) to accept the upgrade on all servers before activating PCA.

Hostname	Upgrade State / Server Status	OAM HA Role / Appl HA Role	Server Role / Network Element	Function	Application Version / Upgrade ISO
DSR-NO2	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0.0-80.18.1
	Norm	N/A	NO_SetupA		
DSR-NO-1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.18.1
	Norm	N/A	NO_SetupA		

5.2 Activation Procedures

This section provides the detailed procedure steps of the feature activation execution.

PCA activation can be performed either

- after all NOAM and SOAM servers are installed and configured. So if the fresh install is for a DSR system with 3 sites, the NOAMs and the SOAMs for all three sites should be installed and configured before performing PCA activation; or
- install and configure only the NOAMs and SOAMs for the first site and activate PCA using 0, then use 0 to activate PCA on additional sites later.

These procedures are executed inside a maintenance window.

The procedures in this section need to be executed in the following order:

- For PCA activation on the entire network:
  - Section 5.2.1 Feature Activation
  - Section 5.2.3 Restart Process
  - Section 5.3.2 System Health Check After Application Activation on NOAM Server
  - Section 5.3.3 System Health Check After Application Activation on SOAM Servers
- For PCA activation on a newly added site:
  - Section 5.2.2 PCA Activation on a Newly Added Site
  - Section 5.2.3 Restart Process
  - Section 5.3.2 System Health Check After Application Activation on NOAM Server
  - Section 5.3.3 System Health Check After Application Activation on SOAM Servers

5.2.1 Feature Activation

PCA Activation on Entire Network

S T E P #	This procedure activates the PCA on complete system. This procedure does not require a Maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish a secure shell session on the active NOAM	Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as the **admusr**. Use your SSH client to connect to the server (ex. Putty). ***Note***: You must consult your own software client's documentation to learn how to launch a connection. For example: `# ssh <active NO XMI VIP Address>`
2. ☐	**PCA Application Activation**: Change directory	Change to the following directory: `$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
3. ☐	**PCA Activation**: Execute the PCA application activation script	Run the feature activation script by executing the following command: `$ ./load.pcaActivationTopLevel` ***Note***: This command execution starts activation on NOAM servers and All Active SOAM servers. Check the /var/TKLC/log/pcaActivationTopLevel.log file to see if there is any execution failure. If the activation fails, then execute the procedure in Section 6.2.3 to restore the system back to state before start of activation.
4. ☐	**PCA Application Activation** (OPTIONAL): Clear the web server cache	Delete all GUI cache files on active SOAM and NOAM for quick view of changes or wait for some time so new changes are reflected. `$ clearCache`

5.2.2 PCA Activation on a Newly Added Site

This procedure needs to be executed only if a new site is added to an existing configured system.

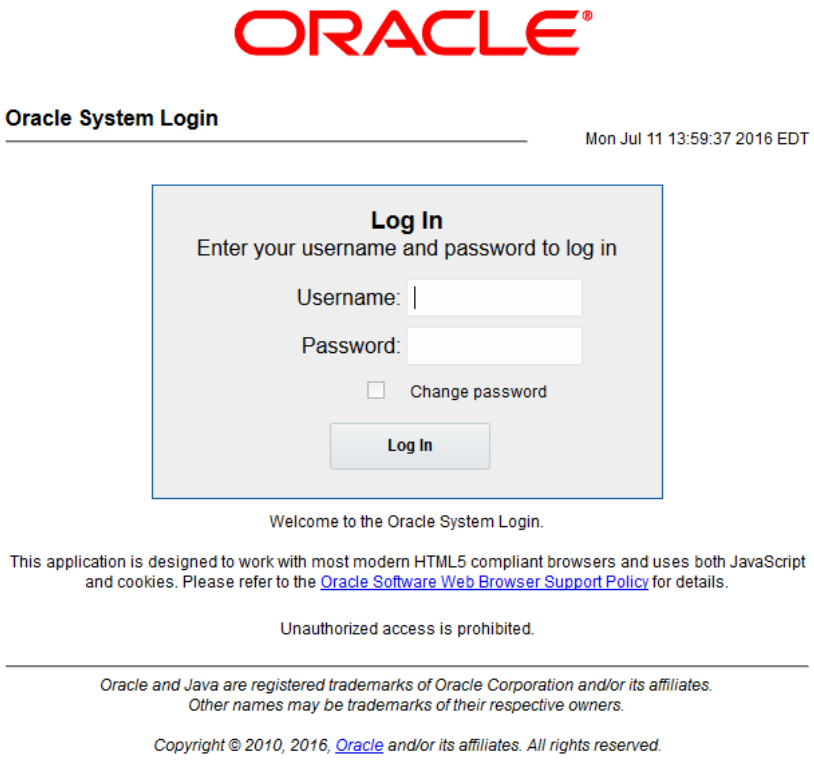
This procedure activates the PCA on newly added site only. This section is only valid if system is already configured and a new site is added to the system at a later stage. **Skip this step if PCA is being activated during a fresh install of the system.**

PCA Activation on Newly Added Site

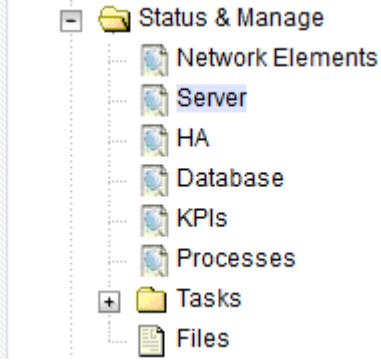
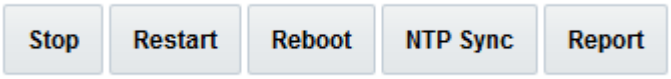
S T E P #	This procedure activates the PCA on a single site newly added to the DSR topology. This procedure does not require a maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance	
1. ☐	Verify configuration of all SOAM servers for the newly added site	Before continuing, verify all SOAM servers should be configured in the topology for the newly added site. 1. Log into the NOAM VIP GUI. 2. Navigate **Status & Manage -> Server**. See all required SOAM servers for the newly added site are configured and Application State is enabled.
2. ☐	Execute the activation procedure	For PCA activation on new site, the activation procedure needs to be executed from the NOAM. Execute the Procedures in Section 5.2.1.

5.2.3 Restart Process

Restart Process

S T E P #	
	This procedure restarts the DSR and SBR application processes. This procedure needs to be performed in a maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: If PCA activation is being performed on a newly added site, this procedure is limited to the servers belonging to that site only. Skip this procedure if PCA is being activated before DA-MP and SBR servers are added to the topology. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

Restart Process

2. ☐	**NOAM VIP**: Restart process on DA-MP servers	Multiple iterations of this step may be executed during the feature activation procedure. This is dependent on the number of DA-MP servers within your system. Make a written record of the number of times the step was performed. It is recommended that no more than 50% of the DA-MPs be restarted at once. Navigate to **Status & Manage -> Server**.  Select the desired DA-MPs, you can use 'Ctrl' to select multiple DA-MPs at once. Click **Restart**.  Click **OK** to confirm. Verify the server changes to the Err state and wait until it returns to the Enabled/Norm state. Repeat for the additional DA-MPs.
3. ☐	**NOAM VIP**: Restart process on SBR servers	Navigate to **Status & Manage -> Server**. Select all the SBR servers, click **Restart** and **OK** to confirm.

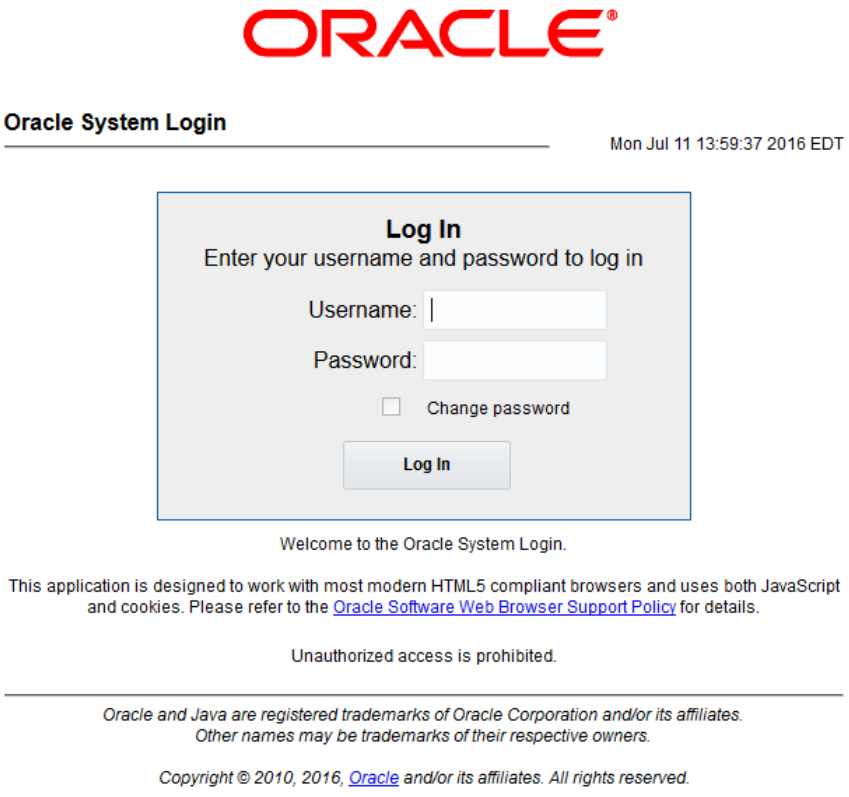
5.3 Post-Activation Procedures

5.3.1 Perform Health Check

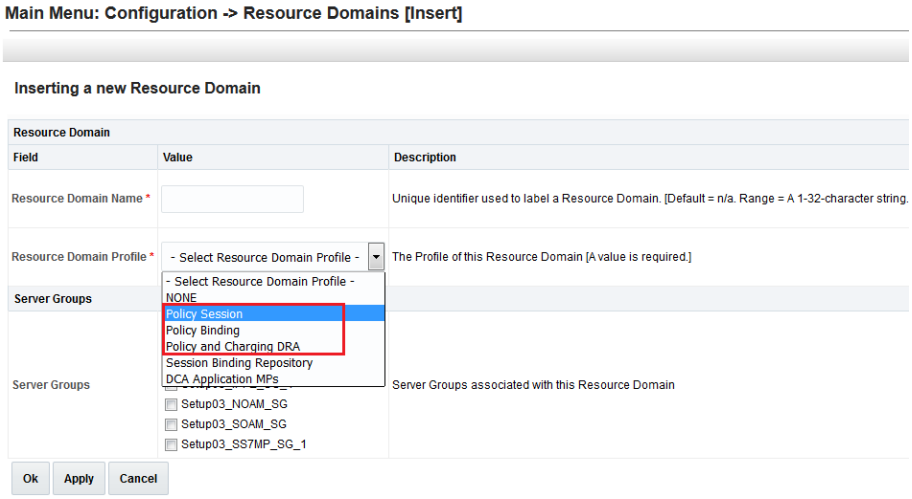
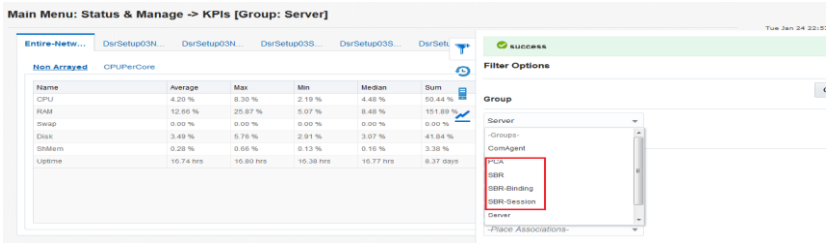
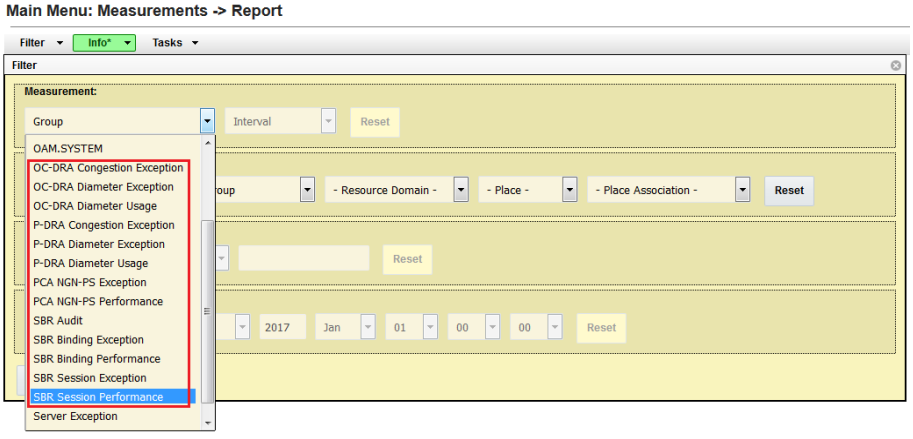
This procedure is used to determine the health and status of the DSR release network and servers.

5.3.2 System Health Check After Application Activation on NOAM Servers

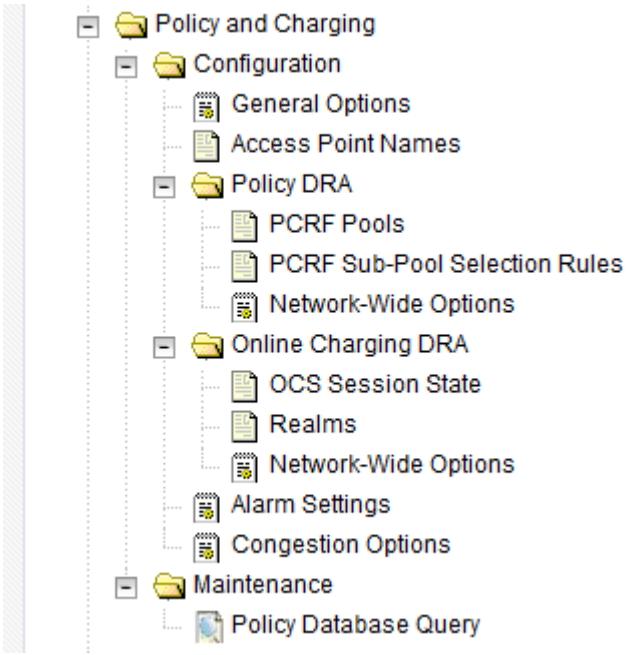
Verification of Application Activation on NOAM Server

S T E P #		
	This procedure verifies the PCA application activation on NOAM server. This procedure does not require a maintenance window Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

Verification of Application Activation on NOAM Server

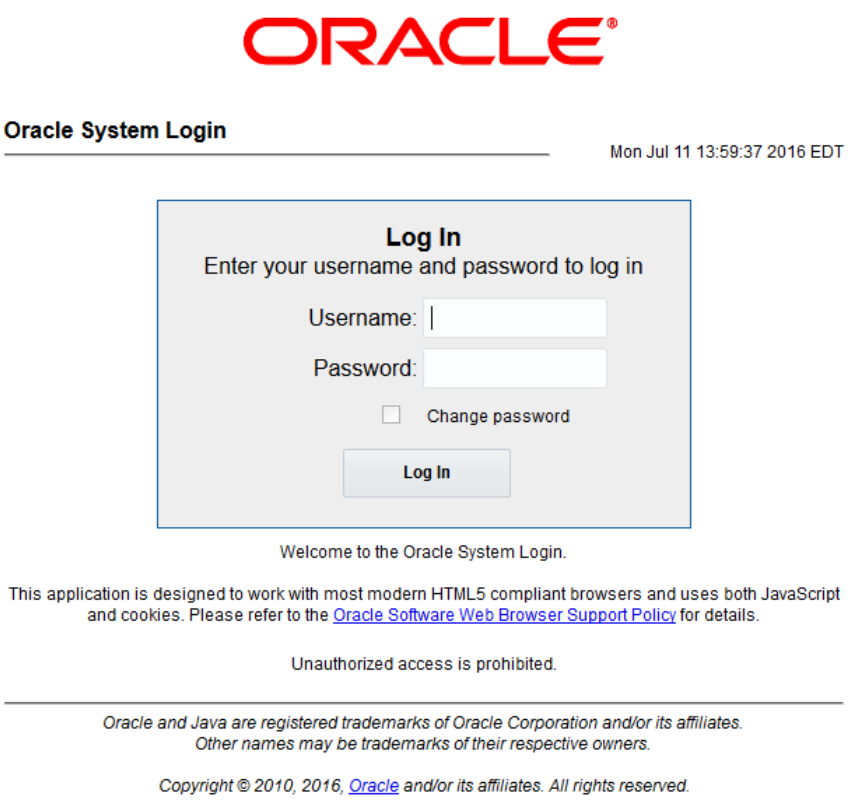
2. ☐	**NOAM VIP**: Verify the Resource Domain Profile shows the new profile entries	Verify the Resource Domain Profile shows the new profile entries. 
3. ☐	**NOAM VIP**: Verify the PCA-specific KPIs are shown	Verify KPI's filter option shows the KPI Group for PCA, SBR-Binding, and SBR-Session. 
4. ☐	**NOAM VIP**: Verify the PCA-specific Measurement groups are shown	Verify Measurement groups are shown for OC-DRA, P-DRA, and SBR. 

Verification of Application Activation on NOAM Server

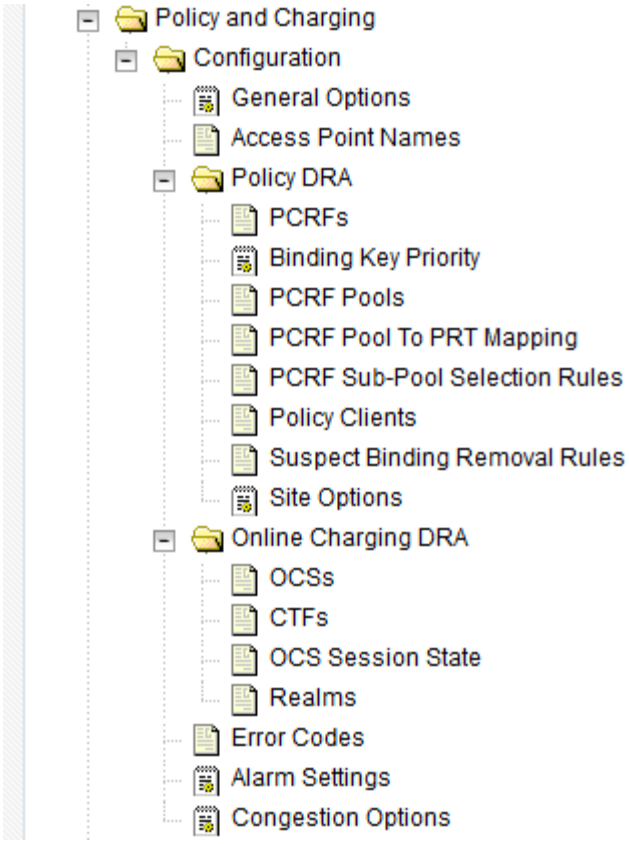
5. ☐	**NOAM VIP**: Verify the Main Menu shows the Policy and Charging submenu	Verify the **Main Menu** on active NOAM shows the Policy and Charging submenu with Configuration and Maintenance screens. 

5.3.3 System Health Check After Application Activation on SOAM Servers

Verification of Application Activation on SOAM Servers

S T E P #	This procedure verifies the activation of PCA on SOAM servers. This procedure does not require a maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**SOAM VIP GUI**: Login	Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

Verification of Application Activation on SOAM Servers

2. ☐	**SOAM VIP**: Verify the Policy and Charging folder is visible in the left hand menu	Verify the Policy and Charging folder appears on the left hand menu: 
3. ☐	**SOAM VIP**: PCA is activated	PCA is activated. Resume the remaining installation/configuration steps.

6. Feature Deactivation

Execute this section only if there is a problem, and it is required to deactivate PCA application and it is desired to revert to the pre-activation version of the software.

6.1 Pre-Deactivation Procedures

Before beginning the feature deactivation, complete this pre-deactivation procedure.

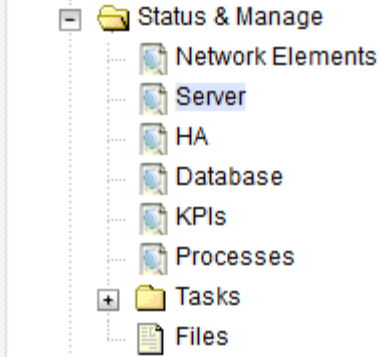
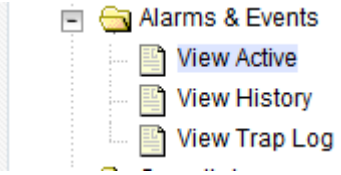
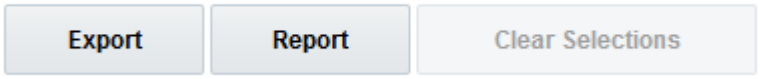
6.1.1 Perform Health Check

This procedure determines the health and status of the DSR network and servers.

Perform Health Check (Pre-Feature Deactivation)

S T E P #		
	This procedure performs needed health checks. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

Perform Health Check (Pre-Feature Deactivation)

2. ☐	**NOAM VIP GUI**: Verify server status	Navigate to **Status & Manage -> Server**.  Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). Appl State | Alm | DB | Reporting Status | Proc Enabled | Norm | Norm | Norm | Norm Enabled | Norm | Norm | Norm | Norm Enabled | Norm | Norm | Norm | Norm
3. ☐	**NOAM VIP GUI**: Log current alarms	Navigate to **Alarms & Events -> View Active**.  Click **Report**.  **Save** or **Print** this report to keep copies for future reference.  Compare this alarm report with those gathered in the pre-activation procedures. Contact My Oracle Support (MOS) if needed.

6.2 Deactivation Procedures

6.2.1 Feature Deactivation

This section provides the detailed steps of the PCA deactivation procedures.

The procedures in this section need to be executed in the following order:

- For PCA deactivation on the entire network
  - Section 6.2.2 Pre PCA Deactivation Steps
  - Section 6.2.3 PCA Deactivation Procedure
  - Section 6.2.5 Post PCA Deactivation Steps
  - Section 6.2.6 Post PCA Deactivation System Health Check
- For PCA deactivation on a site (in the case when the site is being decommissioned)
  - Section 6.2.4 Site Specific PCA Deactivation Procedure
  - Section 6.2.5 Post PCA Deactivation Steps
  - Section 6.2.6.2 System Health Check after Application Deactivation on SOAM Servers

6.2.2 Pre PCA Deactivation Steps

6.2.2.1 Deactivate the GLA Application

Deactivate GLA Application

S T E P #		
	This procedure deactivates the GLA application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Repeat this procedure for all the sites on which GLA deactivation is required. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**SOAM VIP GUI**: Login on the PCA server to be deactivated	Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**SOAM VIP**: Navigate to the Applications screen	Navigate to **Diameter -> Maintenance -> Applications**.
3. ☐	**SOAM VIP**: Deactivate the GLA application	If a GLA record is present on the Applications screen, then execute the steps to deactivate the GLA application as per deactivation procedures defined in [6] DSR GLA Feature Activation Procedure.
4. ☐	**SOAM VIP**: Perform steps on all active SOAM servers	Repeat Step 1-3 on those active SOAM servers on which PCA is activated.

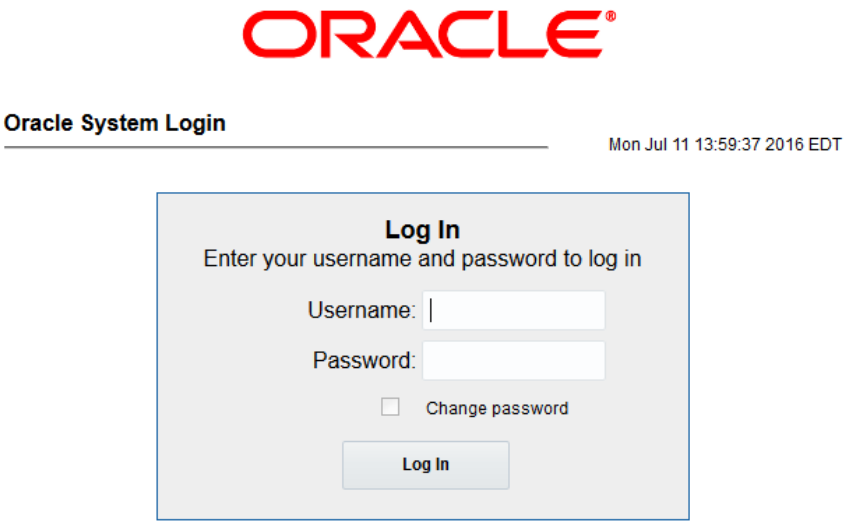
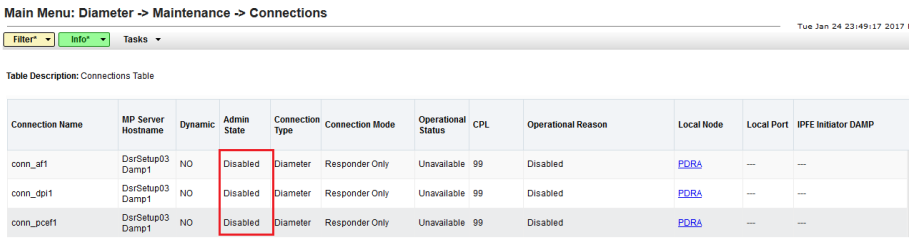
6.2.2.2 Unconfigure PCA Functions

Unconfigure PCA Functions (PDRA and OCDRA)

S T E P #	This procedure unconfigures the PCA functions – Policy DRA and Online Charging DRA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Execution of this procedure causes all Diameter requests routed to the PCA application to be rejected using the Diameter result code configured for Error Condition PCA function unavailable. Before this step, the network operator should take steps to divert policy client and online charging trigger function signaling away from the PCA DSR. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**NOAM VIP**: Unconfigure Policy DRA	Navigate to **Policy and Charging -> Configuration -> General Options**. If Policy DRA is enabled, execute the steps in reference [2], Section 4.7, to unconfigure Policy DRA.
3. ☐	**NOAM VIP**: Unconfigure Online Charging DRA	Navigate to **Policy and Charging -> Configuration -> General Options**. If Online Charging DRA is enabled, execute the steps in reference [2], Section 4.8, to unconfigure Online Charging DRA.

6.2.2.3 Disable Diameter Connections

Disable Diameter Connections

S T E P #	This procedure disables the Diameter connections. This procedure does not require a maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance. ***Note***: Repeat this procedure for all the sites on which PCA deactivation is required.	
1. ☐	**SOAM VIP GUI**: Login	Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**SOAM VIP**: Disable DSR connections	Navigate to **Diameter -> Maintenance -> Connections**. Select all the PCA-specific diameter connections and click **Disable** or click **Disable All** (if applicable). The Admin State of connections should displays as Disabled.  ***Note***: PCA-specific connection includes connections to PCRFs, PCEFs, AFs, CTFs, and OCSes.
3. ☐	**SOAM VIP**: Perform steps on all active SOAM servers	Repeat Steps 1 to 2 on all active SOAM servers on which PCA deactivation is required.

6.2.2.4 Disable Application

Disable Application

S T E P #	This procedure disables the PCA application. This procedure does not require a maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Repeat this procedure for all the sites on which PCA deactivation is required. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**SOAM VIP GUI**: Login	Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**SOAM VIP**: Navigate to Applications screen	Navigate to **Diameter -> Maintenance -> Applications**.
3. ☐	**SOAM VIP**: Disable the PCA application	Select the PCA row and click **Disable**. If there are multiple DA-MPs under this SOAM, then there are multiple entries of PCA in this screen. Select all the entries and click **Disable**.

Disable Application

4. ☐	**SOAM VIP**: Verify the PCA application has been disabled	Navigate to **Diameter -> Maintenance -> Applications**. Verify the Application status has changed to **Disabled**. **Main Menu: Diameter -> Maintenance -> Applications (Filtered)** Filter* Info* **Table Description:** Applications Table Application Name / MP Server Hostname / Admin State / Operational Status / Operational Reason / Congestion Level / Time of Last Update PCA / DsrSetup03 Damp2 / Disabled / Unavailable / Shut Down / Normal / 2017-Jan-24 23:54:05 EST PCA / DsrSetup03 Damp1 / Disabled / Unavailable / Shut Down / Normal / 2017-Jan-24 23:54:05 EST
5. ☐	**SOAM VIP**: Perform steps on all active SOAM servers	Repeat Steps 1 to 4 on all active SOAM servers on which PCA deactivation is required.

6.2.2.5 Remove DSR Configuration Data

Remove DSR Configuration Data

S T E P #		
	This procedure removes the DSR configuration data. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance. **Note**: Do not execute this step if you are going to activate PCA again on this system and you want to re-use the configuration data after re-activation.	
1. ☐	**SOAM VIP GUI**: Login	Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login as the **guiadmin** user: ORACLE **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: Change password Log In Welcome to the Oracle System Login.

Remove DSR Configuration Data

2. ☐	**SOAM VIP**: Remove Application Routing Rules	Navigate to **Diameter -> Configuration -> Application Route Tables**. Select PCA-specific Application Route Table Name. Either click **Delete** to delete the entire table or click **View/Edit Rules,** select PCA-specific Application Route Rules and click **Delete**.
3. ☐	**SOAM VIP**: Remove Peer Routing Rules	Navigate to **Diameter -> Configuration -> Peer Route Tables**. Select PCA-specific Peer Route Table Name. Either click **Delete** to delete the entire table or click **View/Edit Rules,** select PCA-specific Peer Route Rules and click **Delete**.
4. ☐	**SOAM VIP**: Remove Route Lists	Navigate to **Diameter -> Configuration -> Route Lists**. Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
5. ☐	**SOAM VIP**: Remove Route Groups	Navigate to **Diameter -> Configuration -> Route Groups**. Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
6. ☐	**SOAM VIP**: Remove Connections	Navigate to **Diameter -> Configuration -> Connections**. Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen. PCA-specific connection includes connections to PCRFs, PCEFs, AFs, CTFs, and OCSes.
7. ☐	**SOAM VIP**: Remove Peer Nodes	Navigate to **Diameter -> Configuration -> Peer Nodes**. Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
8. ☐	**SOAM VIP**: Remove Local Nodes	Navigate to **Diameter -> Configuration -> Local Nodes**. Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
9. ☐	**SOAM VIP**: Remove CEX Configuration Sets	Navigate to **Diameter -> Configuration -> Configuration Sets -> CEX Configuration Sets**. Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
10. ☐	**SOAM VIP**: Remove CEX parameters	Navigate to **Diameter -> Configuration -> CEX Parameters**. Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
11. ☐	**SOAM VIP**: Remove application IDs	Navigate to **Diameter -> Configuration -> Application IDs**. Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
12. ☐	**SOAM VIP**: Perform steps on all active SOAM servers	Repeat Steps 1 to 11 on all active SOAM servers.

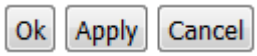
6.2.2.6 Remove Resource Domain Configuration Data

Remove Resource Domain Configuration Data

S T E P #	This procedure removes the Resource Domain configuration data. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as the **guiadmin** user.
2. ☐	**NOAM VIP**: Remove all the data from Place screen as mentioned	Navigate to **Configuration -> Resource Domains**. Delete the Resource Domain of type 'Policy Binding' and 'Policy Session' and 'Policy and Charging DRA' from this screen.

6.2.2.7 Remove Place Associations Configuration Data

Remove Place Associations Configuration Data

S T E P #	This procedure removes the Place Association configuration data. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as the **guiadmin** user.
2. ☐	**NOAM VIP**: Unconfigure the associated Places from the Place Associations as mentioned	Navigate to **Configuration -> Place Associations**. Select the Place Associations of type **Policy and Charging Mated Sites**. Click **Edit**.  Uncheck all the Places associated with this Place Associations and click **OK**.  Repeat this step for all other Place Associations of type **Policy and Charging Mated Sites** and **Policy Binding Region** from this screen.
3. ☐	**NOAM VIP**: Remove all the data from Place Associations screen as mentioned	Navigate to **Configuration -> Place Associations**. Delete the Place Associations of type **Policy and Charging Mated Sites**, and **Policy Binding Region** from this screen.

6.2.2.8 Remove Place Configuration Data

Remove Place Configuration Data

S T E P #	This procedure removes the Place configuration data. Skip this step if places are being used by DCA application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish GUI Session on the NOAM VIP	Establish a GUI session on the NOAM by using the XMI VIP address. Login as the **guiadmin** user.
2. ☐	**NOAM VIP**: Remove all the data from the Places screen as mentioned	Navigate to **Configuration -> Places**. Edit the Places and remove servers from it.

6.2.3 PCA Deactivation Procedure

PCA Application Deactivation

S T E P #	This procedure deactivates the PCA application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Skip this step if PCA is to be activated on a particular site. Execute 0 instead. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish a secure shell session on the active NOAM	Establish an SSH session to the NOAM VIP. Login as the **admusr**.
2. ☐	**PCA Deactivation**: Change directory	Change to the following directory: `$ cd /usr/TKLC/dsr/prod/maint/loaders/deactivate`
3. ☐	**PCA Deactivation**: Execute the PCA application deactivation script	`$ ./load.pcaDeactivationTopLevel` ***Note***: This command execution will starts Deactivation on Active NOAM and all active SOAM servers. Check log file **/var/TKLC/log/pcaDeactivationTopLevel.log** to see if there is any execution failure.
4. ☐	**PCA Deactivation** (Optional): Clear the web server cache	Delete all GUI cache files on active SOAM and NOAM for quick view of changes or wait for some time so new changes can reflect. `$ clearCache`

6.2.4 Site Specific PCA Deactivation Procedure

Execute this section when PCA needs to be deactivated from a particular site.

PCA Application Deactivation on a Particular Site

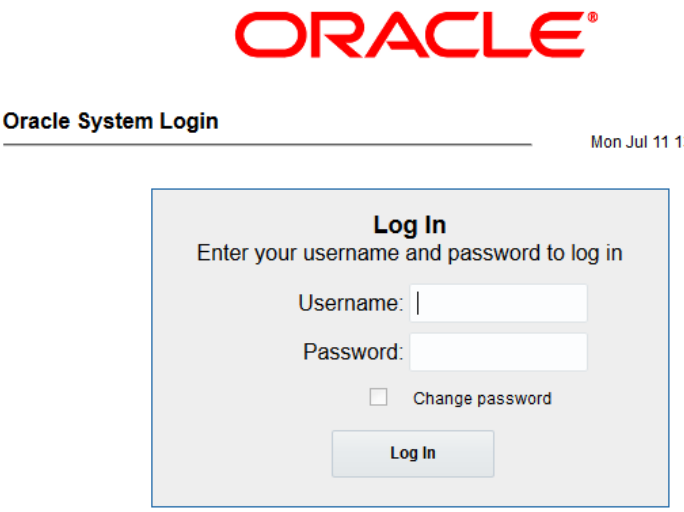
S T E P #	This procedure deactivates the PCA application on a particular site. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish a secure shell session on the active SOAM or on which deactivation is required	Establish an SSH session to the SOAM VIP. Login as the **admusr**.
2. ☐	**PCA Deactivation**: Change directory	Change to the following directory: `$ cd /usr/TKLC/dsr/prod/maint/loaders/deactivate`
3. ☐	**PCA Deactivation**: Execute the PCA application deactivation script	`$ ./load.pcaDeactivateBscoped` ***Note***: This command execution will start Deactivation on selected active SOAM server. Check log file /var/TKLC/log/pcaDeactivateBscoped.log to see if there is any execution failure.
4. ☐	**PCA Deactivation (Optional)**: Clear the web server cache	Delete all GUI cache files on active SOAM and NOAM for quick view of changes or wait for some time so new changes can reflect. `$ clearCache`

6.2.5 Post PCA Deactivation Steps

If PCA Deactivation is being performed on a single site, the procedures in this section apply to the servers belonging to that site only.

6.2.5.1 Move SBR Servers to OOS State

Move SBR Servers to OOS State

S T E P #		
	This procedure puts all the MP servers in SBR Server Groups in OOS. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Please do not execute this step if you are going to activate PCA again on this system and you want to re-use the configuration data after re-activation. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**NOAM VIP**: Navigate to Server Groups screen	Navigate to **Configuration -> Server Groups**.
3. ☐	**NOAM VIP**: Find the server list	Find the servers with Function as **SBR**. ***Note***: SBR can be used for DCA application as well, skip SBR servers being used for DCA application.
4. ☐	**NOAM VIP**: Navigate to HA screen	Navigate to **Status & Manage -> HA**. Edit the servers from list created in Step 3. Change the value of **Max Allowed HA Role** to OOS.

6.2.5.2 Remove SBR Servers from Server Groups

Remove SBR Servers from Server Groups

S T E P #	This procedure removes all the MP servers in SBR Server Groups from their respective Server Groups. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**NOAM VIP**: Navigate to Server Groups screen	Navigate to **Configuration -> Server Groups**.
3. ☐	**NOAM VIP**: Find the server list	Find the servers with Function as SBR, which were configured for PCA. ***Note***: SBR can be used for DCA application as well, skip SBR Server Group being used for DCA application.
4. ☐	**NOAM VIP**: Edit the Server Groups	Navigate to **Configuration -> Server Groups**. Edit the Server Group with **SBR** function and remove the servers from it. Repeat the steps with all server groups with **SBR** function, which are listed in step 3 of this procedure.

6.2.5.3 Delete Server Groups related to SBR

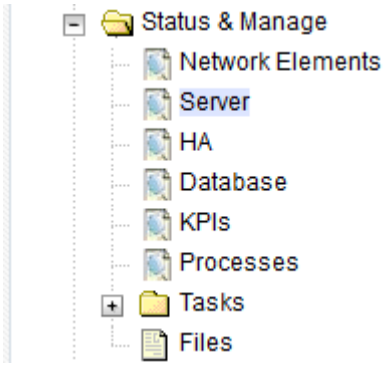
Delete Server Groups related to SBR

S T E P #	This procedure removes the server groups related to SBR. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. **Prerequisite**: Previous procedure has been executed. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**NOAM VIP**: Navigate to Server Groups Screen	Navigate to **Configuration -> Server Groups**.
3. ☐	**NOAM VIP**: Remove Server Groups Resource Domains	Remove the Server Groups, which has Function value **SBR**.

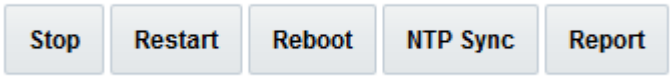
6.2.5.4 Reboot the Servers

Rebooting SBR, DA-MPs, SOAM, and NOAM servers. Use caution while selecting SBR and DA-MP servers. Select SBR and DA-MP servers, which were being used for PCA.

Reboot SBR Servers

S T E P #	This procedure removes the merge data from servers by rebooting them. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Select SBR servers being used for PCA application and for which deactivation done. Skip SBR servers being used for DCA application. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**NOAM VIP**: Navigate to Server Groups Screen	Navigate to **Status & Manage -> Server**. 

Reboot SBR Servers

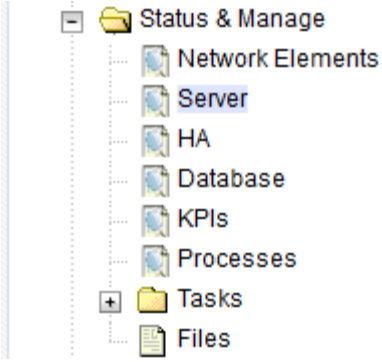
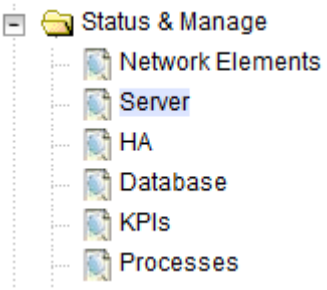
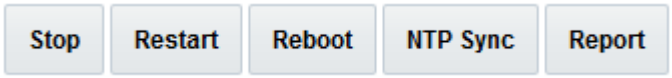
3. ☐	**NOAM VIP**: Reboot the Servers.	Reboots all the relevant SBR servers. Select all the MP servers having Function "SBR" which were being used for PCA application and click **Reboot**.  ***Note***: Skip SBR servers being used for DCA applications. Verify the server changes to the Err state and wait until it returns to the Enabled/Norm state.

Reboot DA-MP Servers

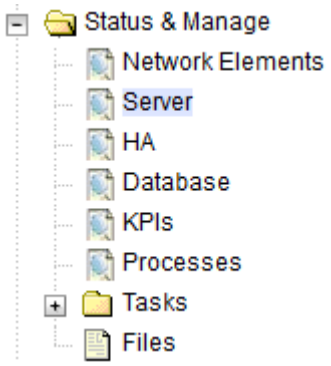
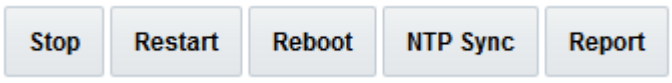
S T E P #	
	This procedure removes the merge data from servers by rebooting them. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Select DA-MP servers being used for PCA application and for which deactivation done. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

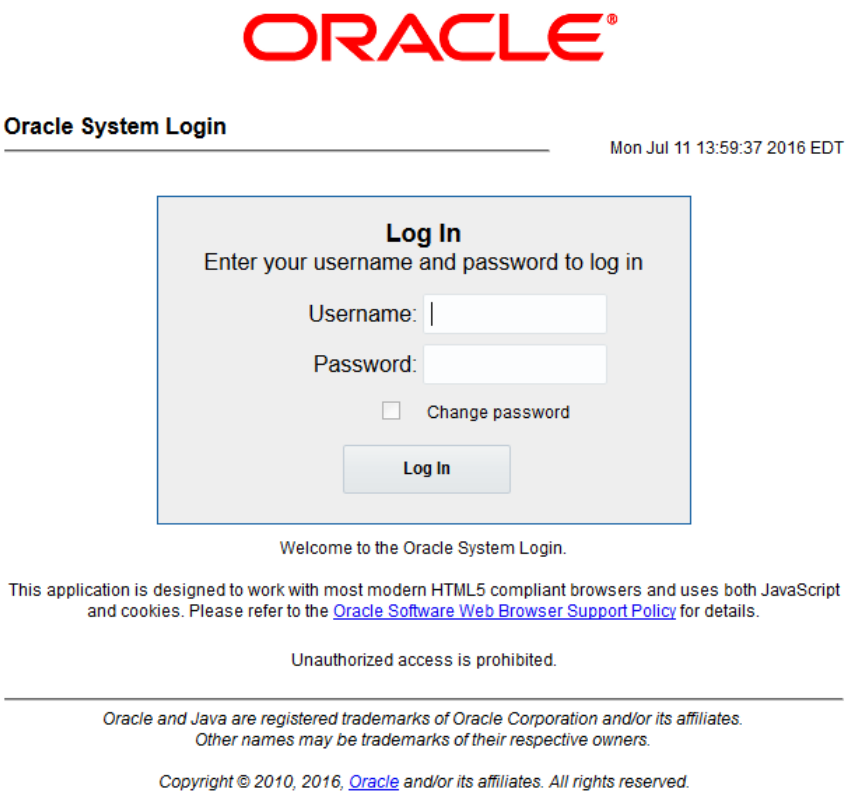
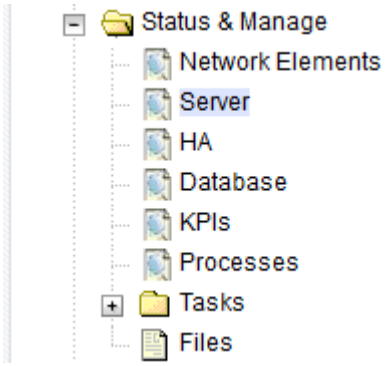
Reboot DA-MP Servers

2. ☐	**NOAM VIP**: Navigate to Server Groups Screen	Navigate to **Status & Manage -> Server**. 
3. ☐	**NOAM VIP**: Reboot the servers	Multiple iterations of this step may be executed during the feature activation procedure. This is dependent on the number of DA-MP servers within your system. Make a written record of the number of times the step was performed. It is recommended that no more than 50% of the DA-MPs be restarted at once. Navigate to **Status & Manage -> Server**.  Select DA-MP servers running PCA. Press **Ctrl** to select multiple DA-MPs at once. Click **Reboot**.  Verify the server changes to the Err state and wait until it returns to the Enabled/Norm state. Repeat for the additional DA-MPs.

Reboot SOAM Servers

S T E P #	This procedure removes the merge data from servers by rebooting them. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Select SOAM servers belonging to the sites running PCA. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**NOAM VIP**: Navigate to Server Groups screen	Navigate to **Status & Manage -> Server** 
3. ☐	**NOAM VIP**: Reboot the servers	Reboots all the relevant SOAM servers. Select all the SOAM servers belonging to sites running PCA and click **Reboot**.  Verify the server changes to the Err state and wait until it returns to the Enabled/Norm state.

Reboot NOAM Servers

S T E P #	This procedure removes the merge data from servers by rebooting them. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 
2. ☐	**NOAM VIP**: Navigate to Server Groups screen	Navigate to **Status & Manage -> Server**. 

Reboot NOAM Servers

3. ☐	**NOAM VIP**: Reboot the servers	Select all NOAM servers except the active NOAM and click **Reboot**. Stop Restart Reboot NTP Sync Report Verify the server changes to the Err state and wait until it returns to the Enabled/Norm state. Select the Active NOAM server and click **Reboot**. Stop Restart Reboot NTP Sync Report After rebooting the active NOAM server, the GUI goes away. Establish a GUI session on the NOAM by using the XMI VIP address. Login as **guiadmin** user after some time.

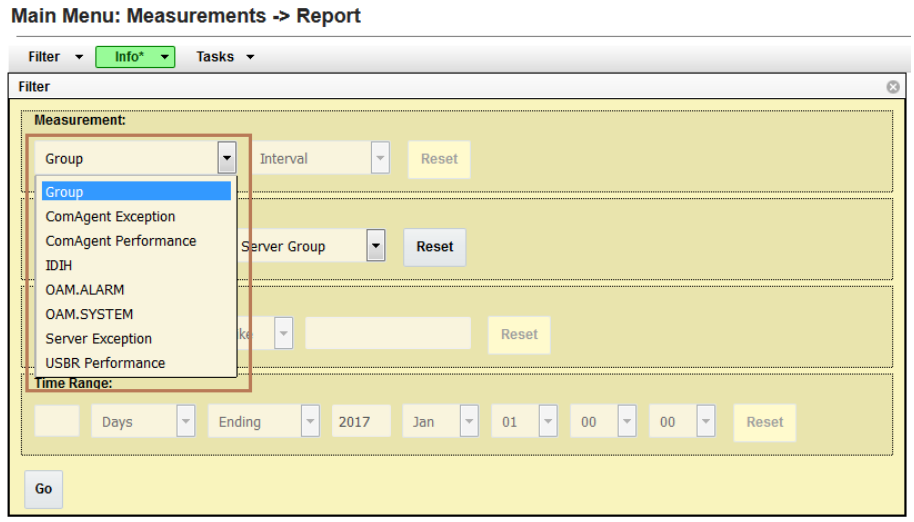
6.2.6 Post PCA Deactivation System Health Check

6.2.6.1 System Health Check after PCA Deactivation on NOAM Server

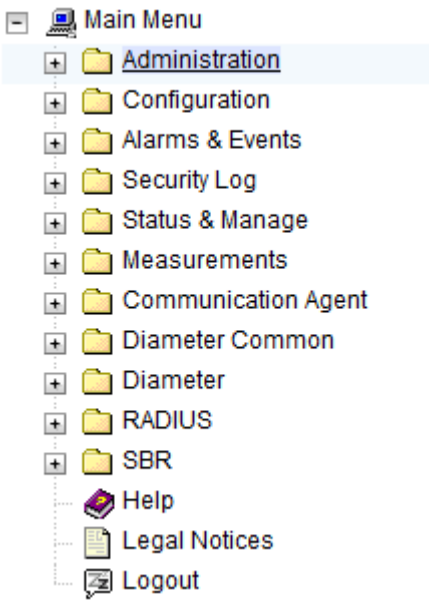
Verification of Application Deactivation on NOAM Server

STEP #	This procedure verifies the PCA application deactivation on NOAM server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. ***Note***: Execute this procedure only when PCA is deactivated on entire network. If PCA is deactivated on a particular site, skip this procedure. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

Verification of Application Deactivation on NOAM Server

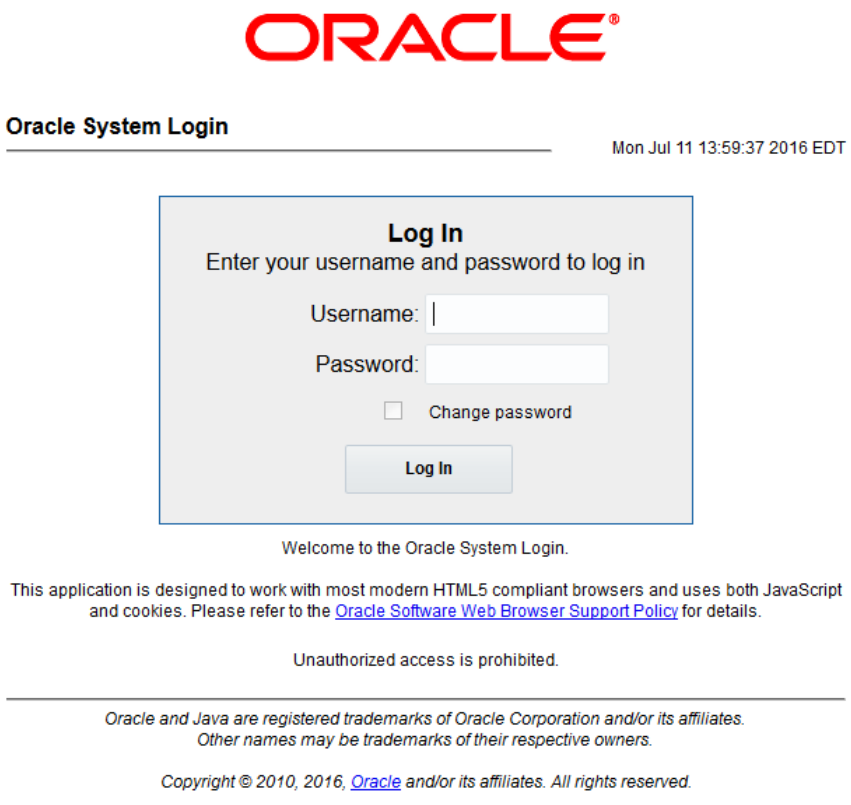
2. ☐	**NOAM VIP**: Verify the Resource Domain Profile does not show the profile entries of Binding and Session profiles	Verify the Resource Domain Profile list does not show the profile entries of **Policy and Charging DRA**, **Policy Session**, and **Policy Binding**. 
3. ☐	**NOAM VIP**: Verify the KPIs are not shown for PCA, SBR-Binding, and SBR-Session	Verify KPIs filter option do not show the KPI groups for PCA, SBR-Binding and SBR-Session. 
4. ☐	**NOAM VIP**: Verify the Measurement groups are not shown for OC-DRA, P-DRA and SBR-Binding, and SBR-Session	Verify Measurement groups are not shown for OC-DRA, P-DRA, SBR-Binding, and SBR-Session. 

Verification of Application Deactivation on NOAM Server

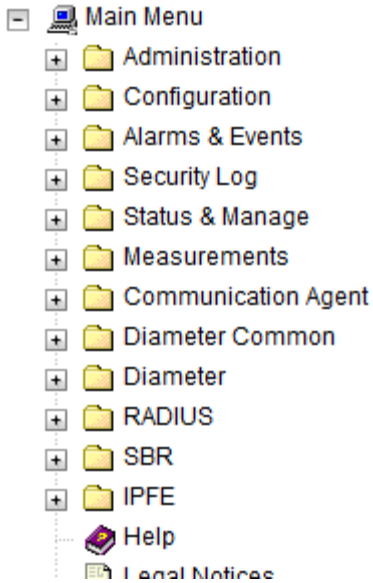
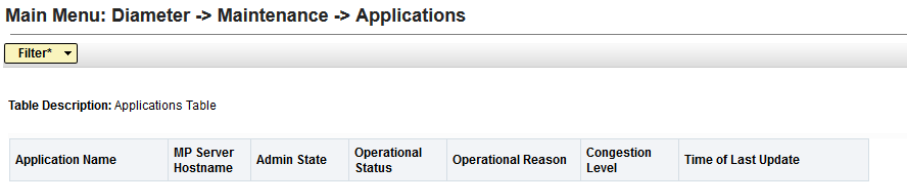
5. ☐	**NOAM VIP**: Verify the Main Menu don't show the Policy and Charging submenu	Verify Main Menu on active NOAM does not show the Policy and Charging submenu. 

6.2.6.2 System Health Check after Application Deactivation on SOAM Servers

Verification of Application Deactivation on SOAM Servers

S T E P #		
	This procedure verifies the PCA application deactivation on SOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**SOAM VIP GUI**: Login	Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter a URL of: `http://<Primary_SOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

Verification of Application Deactivation on SOAM Servers

2. ☐	**SOAM VIP**: Verify the Policy and Charging folder is not visible in the left hand menu	Verify the Policy and Charging folder does not appear on the left hand menu: 
3. ☐	**SOAM VIP**: Verify the Diameter maintenance application menu do not show the entry of PCA application	Verify the Diameter maintenance application menu do not show the entry of PCA application 
4. ☐	**SOAM VIP**: Verify PCA application on all active SOAM servers	Repeat Steps 1 to 3 on all active SOAM servers for which PCA has been deactivated.

6.3 Post-Deactivation Procedures

To complete a deactivation, complete this post-deactivation procedure.

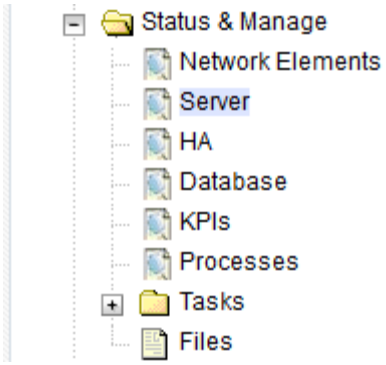
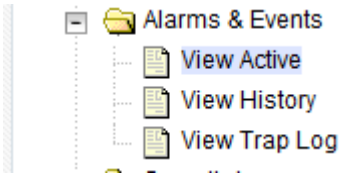
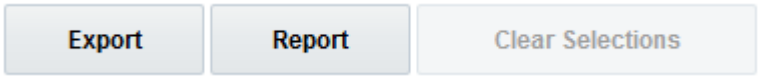
6.3.1 Perform Health Check

This procedure determines the health and status of the network and servers.

Perform Health Check (Post-Feature Deactivation)

S T E P #	This procedure performs a post activation health check. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**NOAM VIP GUI**: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the **guiadmin** user: 

Perform Health Check (Post-Feature Deactivation)

2. ☐	**NOAM VIP GUI**: Verify server status	Navigate to **Status & Manage -> Server**.  Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc). **Appl State** | **Alm** | **DB** | **Reporting Status** | **Proc** Enabled | Norm | Norm | Norm | Norm Enabled | Norm | Norm | Norm | Norm Enabled | Norm | Norm | Norm | Norm
3. ☐	**NOAM VIP GUI**: Log current alarms	Navigate to **Alarms & Events -> View Active**.  Click **Report**.  **Save** or **Print** this report to keep copies for future reference.  Compare this alarm report with those gathered in the pre-Deactivation procedures. Contact My Oracle Support (MOS) if needed.

7. Engineering Notes

FIPS integrity verification test failed: In DSR 7.1+, you may see 'FIPs integrity verification test failed' message displayed during the activation/Deactivation output, this message is expected and harmless.

7.1 Sample Output of Activation (Active NOAM)

```
[admusr@DsrSetup03Noam1 activate]$ ./load.pcaActivationTopLevel
========= Start of Log Data in file /var/TKLC/log/pcaActivationTopLevel.log
==========
====================================S-T-A-R-T=====================================
Log file location: /var/TKLC/log/pcaActivationTopLevel.log
Note:-
In case of any failure please execute
/usr/TKLC/dsr/prod/maint/loaders/deactivate/load.pcaDeactivationTopLevel script to
revert the changes.
================================================================================
Execution of Activation Process Starts
================================================================================
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.pcaActivateAscoped script
on DsrSetup03Noam1
========== Start of Log Data in file /var/TKLC/log/pcaActivateAscoped.log
===========
Server Name  : DsrSetup03Noam1
Server Role  : NETWORK_OAMP
Node Id      : DsrSetup03Noam1
HA State     : Active
Cluster Role : Primary
=============================================
Add PCA to DsrApplication.
=============================================
================================
Verify that PCA is in the table
================================
id=6
name=PCA
unavailableAction=SendAnswer
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=Policy and Charging Application Unavailable Or Degraded
```

```
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=PCA Resource Exhausted
routeListId=65535
realm=
fqdn=
mcl=0
================================
Add PCA KPI group
============================
Add PDRA Measurement groups
========================================
Add Permission Group headers for PCA
========================================
Add Resource Domain Profiles
============================
Add Place Association Types
============================================================
Add mapping between ResourceDomainName to ComAgentResourceId
============================================================
RdName2ComAgentResId do not have any data. So, adding placeholders for comAgentResId
reserved for PCA
  === changed 1 records ===
Taking backup of current system values of ComAgent HA Service timeout configuration.
Setting the ComAgent HA Service timeout configuration values.
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
====================================E-N-D=====================================
Execution status of activation script on DsrSetup03Noam1: PASSED
Please check /var/TKLC/log/pcaActivateAscoped.log for more details.
================================================================================
Starting Activation on StandBy NOAMP Server if it exists in the topology.
DsrSetup03Noam1 is Active and Primary NOAMP Server. So, proceeding with next NOAMP
Server.
================================================================================
```

```
FIPS integrity verification test failed.

Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.pcaActivateStandByAscoped
script on DsrSetup03Noam2

FIPS integrity verification test failed.

======= Start of Log Data in file /var/TKLC/log/pcaActivateStandbyAscoped.log
========

Server Name : DsrSetup03Noam2

Server Role: NETWORK_OAMP

================================================

Add PCA to DsrApplication.

================================================

Verify that PCA is in the table

================================

id=6

name=PCA

unavailableAction=SendAnswer

avpInsertion=Yes

shutdownMode=Graceful

shutdownTimer=5

resultCode=3002

vendorId=0

errorString=Policy and Charging Application Unavailable Or Degraded

resExhResultCode=3004

resExhVendorId=0

resExhErrorString=PCA Resource Exhausted

routeListId=65535

realm=

fqdn=

mcl=0

====================================

Add Permission Group headers for PCA

================================================END=================================
==

Execution status of activation script on DsrSetup03Noam2: PASSED

Please check /var/TKLC/log/pcaActivateStandbyAscoped.log.DsrSetup03Noam2 for more
details.

FIPS integrity verification test failed.

FIPS integrity verification test failed.

pcaActivateStandbyAscoped.log
100% 2218     2.2KB/s   00:00

======= Activation done on all Network OAMP Servers  =======
```

```
======= Starting Activation on System OAM servers =======
DsrSetup03Soam1 is Active. So, proceeding with Activation.
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.pcaActivateBscoped script
on DsrSetup03Soam1
FIPS integrity verification test failed.
============ Start of Log Data in file /var/TKLC/log/pcaActivateBscoped.log
==========
Server Name : DsrSetup03Soam1
Server Role: SYSTEM_OAM
Node Id    : DsrSetup03Soam1
HA State   : Active
================================================
Add PCA to DsrApplication. If already present then skip.
================================================
Verify that PCA is in the table
================================
id=6
name=PCA
unavailableAction=SendAnswer
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=Policy and Charging Application Unavailable Or Degraded
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=PCA Resource Exhausted
routeListId=65535
realm=
fqdn=
mcl=0
============================================================
Add Permission Group headers for PCA
============================================================
FIPS integrity verification test failed.
FIPS integrity verification test failed.
======== Start of Log Data in file /var/TKLC/log/pcaActivateStandbyBscoped.log
=======
```

```
Server Name : DsrSetup03Soam2

Server Role: SYSTEM_OAM

Node Id    : DsrSetup03Soam2

====================================

Add Permission Group headers for PCA

==============================================END=================================
==

Execution status of activation script on DsrSetup03Soam2: PASSED

Please check /var/TKLC/log/pcaActivateStandbyBscoped.log.DsrSetup03Soam2 for more
details.

FIPS integrity verification test failed.

FIPS integrity verification test failed.

==============================================END=================================
==

Execution status of activation script on DsrSetup03Soam1: PASSED

Please check /var/TKLC/log/pcaActivateBscoped.log.DsrSetup03Soam1 for more details.

FIPS integrity verification test failed.

FIPS integrity verification test failed.

pcaActivateBscoped.log
100% 3004     2.9KB/s   00:00

================================================================================

DsrSetup03Soam2 is not Active. Proceeding with next system oam server for activation
process.

================================================================================

Execution of PCA Activation Script complete.

====================================E-N-D=======================================

[admusr@DsrSetup03Noam1 activate]$
```

7.2 Sample Output of Deactivation (Active NOAM)

```
[admusr@DsrSetup03Noam1 deactivate]$ ./load.pcaDeactivationTopLevel

==================== S-T-A-R-T of log pcaDeactivationTopLevel.log
====================

Log file location: /var/TKLC/log/pcaDeactivationTopLevel.log

================================================================================

Execution of Deactivation Process Starts

================================================================================

All policy binding and session data is clean, proceed ahead with PCA deactivation

================================================================================

DsrSetup03Soam1 is Active. So, proceeding with Deactivation.

FIPS integrity verification test failed.

Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/load.pcaDeactivateBscoped
script on DsrSetup03Soam1
```

```
FIPS integrity verification test failed.
========== Start of Log Data in file /var/TKLC/log/pcaDeactivateBscoped.log
==========
Server Name : DsrSetup03Soam1
Server Role: SYSTEM_OAM
Node Id    : DsrSetup03Soam1
HA State   : Active
GLA is not activated, proceed ahead with PCA deactivation
=========================================================
Remove PCA Application from DsrApplicationPerMp table
=========================================================
  === deleted 3 records ===
================================================
Remove PCA Application from DsrApplication table
================================================
  === deleted 1 records ===
============================================================
Remove permission group headers for PCA       on SOAM server
============================================================
  === deleted 1 records ===
  === deleted 1 records ===
FIPS integrity verification test failed.
FIPS integrity verification test failed.
====== Start of Log Data in file /var/TKLC/log/pcaDeactivateStandbyBscoped.log
=======
Server Name : DsrSetup03Soam2
Server Role: SYSTEM_OAM
Node Id    : DsrSetup03Soam2
============================================================
Remove permission group headers for PCA on SOAM server
============================================================
  === deleted 1 records ===
  === deleted 1 records ===
========================================== END
====================================
Execution status of deactivation script on DsrSetup03Soam2: PASSED
Please check /var/TKLC/log/pcaDeactivateStandbyBscoped.log.DsrSetup03Soam2 for more
details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
======================================== END
========================================
```

```
Execution status of deactivation script on DsrSetup03Soam1: PASSED

Please check /var/TKLC/log/pcaDeactivateBscoped.log.DsrSetup03Soam1 for more
details.

FIPS integrity verification test failed.

FIPS integrity verification test failed.

pcaDeactivateBscoped.log
100% 2885     2.8KB/s   00:00

================================================================================

DsrSetup03Soam2 is not Active. Proceeding with next server for de-activation
process.

================================================================================

Starting Deactivation on Standby NOAMP server if present in topology.

================================================================================

DsrSetup03Noam1 is Active NOAMP Server. Proceeding with next NOAMP server in the
list.

================================================================================

FIPS integrity verification test failed.

Executing
/usr/TKLC/dsr/prod/maint/loaders/deactivate/load.pcaDeactivateStandByAscoped script
on DsrSetup03Noam2

FIPS integrity verification test failed.

=====================  S-T-A-R-T of log pcaDeactivateAscoped.log
=====================

Server Name : DsrSetup03Noam2

Server Role : NETWORK_OAMP

================================================

Remove PCA Application from DsrApplication table

================================================

  === deleted 1 records ===

============================================

Remove permission group headers for PCA

============================================

  === deleted 1 records ===

  === deleted 1 records ===

====================================E-N-D=======================================

Execution status of deactivation script on DsrSetup03Noam2: PASSED

Please check /var/TKLC/log/pcaDeactivateAscoped.log.DsrSetup03Noam2 for more
details.

FIPS integrity verification test failed.

FIPS integrity verification test failed.

pcaDeactivateAscoped.log
100%  963     0.9KB/s   00:00

================================================================================

 Starting Deactivation on Active NOAMP server.
```

```
================================================================================
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/load.pcaDeactivateAscoped
script on DsrSetup03Noam1
========== Start of Log Data in file /var/TKLC/log/pcaDeactivateAscoped.log
==========
Server Name  : DsrSetup03Noam1
Server Role  : NETWORK_OAMP
Node Id      : DsrSetup03Noam1
HA State     : Active
Cluster Role : Primary
GLA is not activated, proceed ahead with PCA deactivation
All policy binding and session data is clean, proceed ahead with PCA deactivation
==============================
Remove PCA and pSBR KPI groups
==============================
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
========================================
Remove PDRA and PSBR  Measurement groups
========================================
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
============================================
Remove permission group headers for PCA
============================================
  === deleted 1 records ===
  === deleted 1 records ===
================================================
Remove PCA from DsrApplicationPerMp table
================================================
```

```
  === deleted 0 records ===
================================================
Remove PCA Application from DsrApplication table
================================================
  === deleted 1 records ===
============================
Remove routing profile data
============================
  === deleted 1 records ===
  === deleted 1 records ===
================================
Remove Psbr capacity constraints
================================
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
================================================================================
Remove  data for mapping between ResourceDomainName to ComAgentResourceId
 reserved for policy binding and session profiles
================================================================================
  === deleted 66 records ===
================================
Remove Resource Domain Profiles
================================
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
========================================
Remove Place Association data
========================================
Remove Place Association Types
================================
  === deleted 1 records ===
  === deleted 1 records ===
======================================
Set HandleProtocolErrorAnswers flag in LongParam to default(No)
  === changed 1 records ===
======================================
/var/TKLC/db/filemgmt/TempPcaActivationDataFile.log exists. Reading ComAgent
Configuration data from it.
```

```
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
  === changed 1 records ===
========================================= END
=====================================
Execution status of deactivation script on DsrSetup03Noam1: PASSED
================================================================================
Execution of PCA Deactivation Script complete.
=====================================E-N-D=======================================
[admusr@DsrSetup03Noam1 deactivate]$
```

Appendix A. PCA Activation on Active/Standby NOAM and SOAM Server

The following procedures activate PCA on active/standby NOAM and SOAM servers. Follow the appropriate procedure as needed for your disaster recovery.

Note: These procedures need to be executed during disaster recovery and are not part of installation.

Appendix A.1 PCA Activation on Active NOAM

PCA Activation on Active NOAM Server

S T E P #	This procedure activates the PCA on a NOAM system. This procedure does not require a Maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish a secure shell session on the active NOAM	Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as the **admusr**. Use your SSH client to connect to the server (ex. Putty). ***Note***: You must consult your own software client's documentation to learn how to launch a connection. For example: `# ssh <active NO XMI VIP Address>`
2. ☐	**PCA Application Activation**: Change directory	Change to the following directory: `$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
3. ☐	**PCA Activation**: Execute the PCA application activation script	Run the feature activation script by executing the following command: `$ ./load.pcaActivateAscoped` Check the /var/TKLC/log/pcaActivateAscoped.log file to see if there is any execution failure. If the activation fails, then execute the procedure in Section 6.2.3 to restore the system back to state before start of activation.

PCA Activation on Active NOAM Server

4. ☐	**PCA Application Activation** (OPTIONAL): Clear the web server cache	Delete all GUI cache files on active NOAM for quick view of changes or wait for some time so new changes are reflected. `$ clearCache`

Appendix A.1.1 Sample Output of Activation (Active NOAM)

```
[admusr@NO2 activate]$ ./load.pcaActivateAscoped
========== Start of Log Data in file /var/TKLC/log/pcaActivateAscoped.log
===========
Server Name  : NO2
Server Role  : NETWORK_OAMP
Node Id      : NO2
HA State     : Active
Cluster Role : Primary
================================================
Add PCA to DsrApplication.
================================================
Verify that PCA is in the table
================================
id=6
name=PCA
unavailableAction=SendAnswer
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=Policy and Charging Application Unavailable Or Degraded
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=PCA Resource Exhausted
routeListId=65535
realm=
fqdn=
mcl=0
================================
Add PCA KPI group
==================
Add PDRA Measurement groups
```

```
==========================

Add Permission Group headers for PCA & SBR

========================================

Add Resource Domain Profiles

==========================

Add Place Association Types

============================================================

Add mapping between ResourceDomainName to ComAgentResourceId

============================================================

RdName2ComAgentResId do not have any data. So, adding placeholders for comAgentResId
reserved for PCA

====================================

Add PSBR record in AppProcControl table

====================================

  === changed 1 records ===

Taking backup of current system values of ComAgent HA Service timeout configuration.

Setting the ComAgent HA Service timeout configuration values.

  === changed 1 records ===

  === changed 1 records ===

  === changed 1 records ===

  === changed 1 records ===

  === changed 1 records ===

  === changed 1 records ===

  === changed 1 records ===

====================================E-N-D=======================================
```

Appendix A.2 PCA Activation on Standby NOAM

PCA Activation on Standby NOAM Server

S T E P #	This procedure activates the PCA on a NOAM system. This procedure does not require a Maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish a secure shell session on the active NOAM	Establish a secure shell session on the standby NOAM by using the XMI VIP address. Login as the **admusr**. Use your SSH client to connect to the server (ex. Putty). ***Note***: You must consult your own software client's documentation to learn how to launch a connection. For example: `# ssh <active NO XMI VIP Address>`

PCA Activation on Standby NOAM Server

2. ☐	**PCA Application Activation**: Change directory	Change to the following directory: `$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
3. ☐	**PCA Activation**: Execute the PCA application activation script	Run the feature activation script by executing the following command: `$ ./load.pcaActivateStandByAscoped` ***Note***: This command execution starts activation on NOAM servers and All Active SOAM servers. Check the /var/TKLC/log/pcaActivateStandbyAscoped.log file to see if there is any execution failure. If the activation fails, then execute the procedure in Section 6.2.3 to restore the system back to state before start of activation.
4. ☐	**PCA Application Activation** (OPTIONAL): Clear the web server cache	Delete all GUI cache files on active NOAM for quick view of changes or wait for some time so new changes are reflected. `$ clearCache`

Appendix A.2.1 Sample Output of Activation (Standby NOAM)

```
[admusr@NO1 activate]$ ./load.pcaActivateStandByAscoped
======= Start of Log Data in file /var/TKLC/log/pcaActivateStandbyAscoped.log
========
Server Name : NO1
Server Role: NETWORK_OAMP
================================================
Add PCA to DsrApplication.
================================================
Verify that PCA is in the table
================================
id=6
name=PCA
unavailableAction=SendAnswer
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=Policy and Charging Application Unavailable Or Degraded
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=PCA Resource Exhausted
```

```
routeListId=65535
realm=
fqdn=
mcl=0
====================================
Add Permission Group headers for PCA
=====================================================END=============================
==
```

Appendix A.3 PCA Activation on Active SOAM

PCA Activation on Active SOAM Server

S T E P #	This procedure activates the PCA on an SOAM system. This procedure does not require a Maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish a secure shell session on the active SOAM	Establish a secure shell session on the active SOAM by using the XMI VIP address. Login as the **admusr**. Use your SSH client to connect to the server (ex. Putty). ***Note***: You must consult your own software client's documentation to learn how to launch a connection. For example: `# ssh <active SOAM XMI VIP Address>`
2. ☐	**PCA Application Activation**: Change directory	Change to the following directory: `$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
3. ☐	**PCA Activation**: Execute the PCA application activation script	Run the feature activation script by executing the following command: `$ ./load.pcaActivateBscoped` Check the /var/TKLC/log/pcaActivateBscoped.log file to see if there is any execution failure. If the activation fails, then execute the procedure in Section 6.2.3 to restore the system back to state before start of activation.
4. ☐	**PCA Application Activation** (OPTIONAL): Clear the web server cache	Delete all GUI cache files on active SOAM for quick view of changes or wait for some time so new changes are reflected. `$ clearCache`

Appendix A.3.1 Sample Output of Activation (Active SOAM)

```
[admusr@SO1 activate]$ ./load.pcaActivateBscoped
========== Start of Log Data in file /var/TKLC/log/pcaActivateBscoped.log
==========
Server Name : SO1
```

```
Server Role: SYSTEM_OAM
Node Id    : SO1
HA State   : Active
=============================================
Add PCA to DsrApplication. If already present then skip.
=============================================
Verify that PCA is in the table
================================
id=6
name=PCA
unavailableAction=SendAnswer
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=Policy and Charging Application Unavailable Or Degraded
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=PCA Resource Exhausted
routeListId=65535
realm=
fqdn=
mcl=0
=========================================================
Add Permission Group headers for PCA & SBR on SOAM server
=========================================================
FIPS integrity verification test failed.
FIPS integrity verification test failed.
======= Start of Log Data in file /var/TKLC/log/pcaActivateStandbyBscoped.log
========
Server Name : SO2
Server Role: SYSTEM_OAM
Node Id    : SO2
HA State   : Stby
====================================
Add Permission Group headers for PCA
=============================================END=================================
==
Execution status of activation script on SO2: PASSED
```

```
Please check /var/TKLC/log/pcaActivateStandbyBscoped.log.SO2 for more details.

FIPS integrity verification test failed.

FIPS integrity verification test failed.

pcaActivateStandbyBscoped.log
100%  785     0.8KB/s   00:00

==========================================END=================================
==
```

Appendix A.4 PCA Activation on Standby SOAM

PCA Activation on Standby SOAM Server

S T E P #	This procedure activates the PCA on an SOAM system. This procedure does not require a Maintenance window. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Establish a secure shell session on the active SOAM	Establish a secure shell session on the active SOAM by using the XMI VIP address. Login as the **admusr**. Use your SSH client to connect to the server (ex. Putty). ***Note***: You must consult your own software client's documentation to learn how to launch a connection. For example: `# ssh <active SOAM XMI VIP Address>`
2. ☐	**PCA Application Activation**: Change directory	Change to the following directory: `$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
3. ☐	**PCA Activation**: Execute the PCA application activation script	Run the feature activation script by executing the following command: `$ ./load.pcaActivateStandByBscoped` Check the /var/TKLC/log/pcaActivateStandbyBscoped.log file to see if there is any execution failure. If the activation fails, then execute the procedure in Section 6.2.3 to restore the system back to state before start of activation.
4. ☐	**PCA Application Activation** (OPTIONAL): Clear the web server cache	Delete all GUI cache files on active SOAM for quick view of changes or wait for some time so new changes are reflected. `$ clearCache`

Appendix A.4.1 Sample Output of Activation (Standby SOAM)

```
[root@SO2 activate]# ./load.pcaActivateStandByBscoped

======= Start of Log Data in file /var/TKLC/log/pcaActivateStandbyBscoped.log
========

Server Name : SO2

Server Role: SYSTEM_OAM
```

```
Node Id    : SO2
HA State   : Stby
=====================================
Add Permission Group headers for PCA
=================================================END=============================
[root@SO2 activate]#
```

Appendix B. My Oracle Support (MOS)

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. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:

   For technical issues such as creating a new Service Request (SR), select 1.

   For non-technical issues such as registration or assistance with MOS, select 2.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.