

# Oracle® Communications

## Diameter Signaling Router Policy and Charging Application Feature Activation Guide



Release 9.0.0.0.0

F79977-01

April 2023

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

F79977-01

Copyright © 2000, 2023, Oracle and/or its affiliates.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

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

# Contents

<b>1</b>	<b>Introduction</b>	
1.1	Purpose and Scope	1-1
1.2	References	1-1
<b>2</b>	<b>PCA Feature Activation Overview</b>	
2.1	Definition of Activation for the PCA Feature	2-1
2.2	Preactivation Overview	2-2
2.3	Activation Procedures	2-2
2.4	Post-Feature Activation Overview	2-3
<b>3</b>	<b>Feature Deactivation Overview</b>	
3.1	Pre-Feature Deactivation Overview	3-1
3.2	Feature Deactivation Execution Overview	3-2
3.3	Post-Feature Deactivation Overview	3-3
<b>4</b>	<b>Feature Activation Preparation</b>	
4.1	System Topology Check	4-1
4.2	Perform Health Check	4-3
<b>5</b>	<b>Feature Activation</b>	
5.1	Pre-Activation Procedures	5-1
5.1.1	Health Check for Pre-activation	5-1
5.2	Activation Procedures	5-6
5.2.1	Feature Activation	5-6
5.2.2	PCA Activation on a Newly Added Site	5-7
5.2.3	Restart Process	5-8
5.3	Post-Activation Procedures	5-9
5.3.1	System Health Check After Application Activation on NOAM Servers	5-9

## 6 Feature Deactivation

---

6.1	Pre-Deactivation Procedures	6-1
6.1.1	Health Check for Pre-Deactivation	6-1
6.2	Deactivation Procedures	6-3
6.2.1	Feature Deactivation Procedure	6-3
6.2.2	Pre PCA Deactivation Steps	6-4
6.2.2.1	Deactivate the GLA Application	6-4
6.2.2.2	Unconfigure PCA Functions	6-5
6.2.2.3	Disable Diameter Connections	6-6
6.2.2.4	Disable Application	6-8
6.2.2.5	Remove DSR Configuration Data	6-9
6.2.2.6	Remove Resource Domain Configuration Data	6-11
6.2.2.7	Remove Place Associations Configuration Data	6-11
6.2.2.8	Remove Place Configuration Data	6-12
6.2.3	PCA Deactivation Procedure	6-12
6.2.4	Site Specific PCA Deactivation Procedure	6-13
6.2.5	Post PCA Deactivation Steps	6-13
6.2.5.1	Move SBR Servers to OOS State	6-13
6.2.5.2	Remove SBR Servers from Server Groups	6-15
6.2.5.3	Delete Server Groups related to SBR	6-16
6.2.5.4	Reboot the Servers	6-17
6.2.6	Post PCA Deactivation System Health Check	6-24
6.2.6.1	System Health Check after PCA Deactivation on NOAM Server	6-24
6.2.6.2	System Health Check after Application Deactivation on SOAM Servers	6-27
6.3	Post-Deactivation Procedures	6-29
6.3.1	Health Check for Post-Feature Deactivation	6-29

## 7 Engineering Notes

---

7.1	Sample Output of Activation (Active NOAM)	7-1
7.2	Sample Output of Deactivation (Active NOAM)	7-5

## Part I PCA Activation on Active/Standby NOAM and SOAM Server

---

### A PCA Activation on Active NOAM

---

B PCA Activation on Standby NOAM

---

C PCA Activation on Active SOAM

---

D PCA Activation on Standby SOAM

---

---

# My Oracle Support

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

Call the Customer Access Support 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 My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

# Acronyms

An alphabetized list of acronyms used in the document:

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
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

---

# What's New in this Guide

This section introduces the documentation updates for release 9.0.0.0.0.

**Release 9.0.0.0.0 - F79977-01, April 2023**

No updates made to this document.



# 1

## Introduction

Policy and Charging Application (PCA) features can be activated on a DSR network element (NE).

### 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). These procedures can be performed 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. For deactivation procedures, see [Feature Deactivation Overview](#).

PCA configuration following activation is beyond the scope of this document. For information about PCA configuration postactivation, see *PCA User Guide*.

No additional software installation is required before performing this procedure. The standard DSR installation procedure has loaded all the required software even if the PCA feature is activated later.

### 1.2 References

- *DSR Software Installation and Configuration Procedure 2/2*
- *DSR Policy Charging Application User Guide*
- *DSR PDRA Configuration Work Instruction, WI006808*
- *DSR PDRA Activation/Deactivation Work Instruction, WI006835*
- *DSR PCA Activation and Configuration*
- *DSR GLA Feature Activation Procedure*
- *DSR Software Upgrade Guide*

# 2

## PCA Feature Activation Overview

This section lists the required materials and information required to activate the PCA feature. In addition, [Table 2-1](#) through [Table 3-3](#) provide estimates of the time required to perform the procedures. These tables can be used to estimate the total time required to complete the feature activation. The timing values shown are estimates only – use these tables to plan the timing of the activation, not to perform the procedure. The detailed procedure is described in [Feature Activation](#).

### 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.

**⚠ WARNING:**

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 Preactivation Overview

The preactivation procedures shown in the following table can be performed outside a maintenance window if required. 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 2-1 Preactivation Overview**

Procedure	Elapsed Time (Hours:Minutes)		Feature Activation Prerequisites
	This Step	Cumulative	
<a href="#">System Topology Check</a>	0:00-1:00	0:00-1:00	<ul style="list-style-type: none"> <li>• Verify Network Element Configuration data.</li> <li>• Verify Server Group Configuration data.</li> <li>• Analyze and plan DA-MP restart sequence.</li> </ul>
<a href="#">Perform Health Check</a>	0:01-0:20	1:01-1:20	<ul style="list-style-type: none"> <li>• Verify server status.</li> <li>• Log all current alarms.</li> </ul>

## 2.3 Activation Procedures

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 2-2 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	<ul style="list-style-type: none"> <li>Verify all servers in the network are on the same DSR release.</li> <li>Verify proper PCA feature state.</li> <li>Verify server status.</li> <li>Verify server and server group configurations.</li> <li>Log all current alarms.</li> </ul>
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	<ul style="list-style-type: none"> <li>Log out of NOAM/SOAM GUI.</li> <li>SSH to active NOAM.</li> <li>Login as the <code>admusr</code>.</li> <li>Change directory to <code>/usr/TKLC/dsr/prod/maint/loaders/activate</code>.</li> <li>Execute the feature activation script.</li> <li>Log into NOAM or SOAM GUI.</li> <li>Verify the Policy and Charging folder.</li> <li>Verify Maintenance screen.</li> <li>Log into NOAM GUI (Optional).</li> <li>Restart each active DA-MP server.</li> <li>Verify Maintenance screen.</li> </ul>
Restart Process (0)			<ul style="list-style-type: none"> <li>Restart process on DA-MP servers.</li> <li>Restart process on SBR servers.</li> </ul>

## 2.4 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 2-3 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	<ul style="list-style-type: none"> <li>• Establish GUI session on the NOAM VIP.</li> <li>• Verify the KPIs.</li> <li>• Verify the Measurements.</li> <li>• Verify GUI left hand menu item.</li> </ul>
Perform Health Check (0)	0:01-0:05	0:02-0:10	<ul style="list-style-type: none"> <li>• Establish GUI session on the SOAM VIP.</li> <li>• Verify GUI left hand menu item.</li> </ul>

# 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 3-1 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	<ul style="list-style-type: none"> <li>Establish GUI session on the SOAM VIP.</li> <li>Verify GUI left hand menu item.</li> <li>Establish GUI session on the NOAM VIP.</li> <li>Verify server status.</li> <li>Log current alarms.</li> </ul>
Verify PCA application state and deactivate GLA (0)	00:01-00:05	0:02-0:10	<ul style="list-style-type: none"> <li>Establish GUI session on the SOAM VIP.</li> <li>Verify PCA record in <b>Diameter -&gt; Maintenance -&gt; Applications.</b></li> <li>Verify GLA record in <b>Diameter -&gt; Maintenance -&gt; Applications.</b></li> <li>Deactivate GLA, if activated.</li> </ul>
Unconfigure PCA Functions (PDRA and OCDRA) (0)	00:10-00:40	0:12-0:50	<ul style="list-style-type: none"> <li>Establish GUI session on the NOAM VIP.</li> <li>Unconfigure PDRA function.</li> <li>Unconfigure OCDRA function.</li> </ul>

**Table 3-1 (Cont.) Pre-Feature Deactivation Overview**

Procedure	Elapsed Time (Hours:Minutes)		Pre-Feature Deactivation Procedures
	This Step	Cum.	
Disable Diameter Connections (0)	00:01-00:05	0:13-0:55	<ul style="list-style-type: none"> <li>Establish GUI session on the SOAM VIP.</li> <li>Disable PCA-specific diameter connection.</li> </ul>
Disable application (0)	00:01-00:05	0:14-1:00	<ul style="list-style-type: none"> <li>Establish GUI session on the SOAM VIP.</li> <li>Disable PCA application.</li> </ul>
Remove DSR configuration data (0)	00:01-00:05	0:15-1:05	<ul style="list-style-type: none"> <li>Establish GUI session on the SOAM VIP.</li> <li>Remove PCA-specific DSR configuration.</li> </ul>
Remove Resource Domain configuration data (0)	00:01-00:05	0:16-1:10	<ul style="list-style-type: none"> <li>Establish GUI session on the NOAM VIP.</li> <li>Remove PCA-specific resource domain configuration.</li> </ul>
Remove Place Associations configuration data (0)	00:01-00:05	0:17-1:15	<ul style="list-style-type: none"> <li>Establish GUI session on the NOAM VIP.</li> <li>Remove Place Association configuration.</li> </ul>
Remove Place configuration data (0)	00:01-00:05	0:18-1:20	<ul style="list-style-type: none"> <li>Establish GUI session on the NOAM VIP.</li> <li>Remove Place configuration.</li> </ul>

## 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 3-2 Feature Deactivation Execution 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	<ul style="list-style-type: none"> <li>Log out of active NOAM/SOAM GUI.</li> <li>SSH into active NOAM.</li> <li>Login as the <code>admusr.</code></li> <li>Change directory to <code>/usr/TKLC/dsr/prod/maint/loaders/deactivate</code></li> <li>Execute the feature deactivation script.</li> <li>Log into NOAM or SOAM GUI</li> <li>Verify the Policy and Charging folder.</li> <li>Log into NOAM GUI</li> <li>Restart each active DA-MP server.</li> <li>Verify Maintenance screen.</li> </ul>

## 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 3-3 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	<ul style="list-style-type: none"> <li>Establish GUI session on the NOAM VIP</li> <li>Move SBR server to OOS</li> </ul>
Remove SBR Servers from Server Groups (0)	0:01-0:05	0:02-0:10	<ul style="list-style-type: none"> <li>Establish GUI session on the NOAM VIP</li> <li>Remove SBR server from server group</li> </ul>



**Table 3-3 (Cont.) Post-Feature Deactivation Overview**

Procedure	Elapsed Time (Hours:Minutes)		Post Feature Deactivation Procedures
	This Step	Cum.	
Reboot the Servers (0)	0:10-1:00	0:12-1:05	<ul style="list-style-type: none"> <li>Identify the sequence of the server to be rebooted</li> <li>Reboot the server in sequence</li> </ul>
Perform Health 0, 0, and 0)	0:01-0:05	0:01-0:20	<ul style="list-style-type: none"> <li>Verify server status.</li> <li>Log all current alarms.</li> <li>Verify the KPIs.</li> <li>Verify the Measurements.</li> <li>Verify GUI menu does not shows PCA sub-menu</li> </ul>

# 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

#### Procedure 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.

1. Log in to the NOAM VIP GUI, establish a GUI session on the NOAM server by using the VIP address of the NOAM server.
2. Open the web browser and enter the URL, `http://<Primary_NOAM_VIP_IP_Address>`
3. Log in as the `guiadmin` user.

**Figure 4-1 Oracle System Login**

**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

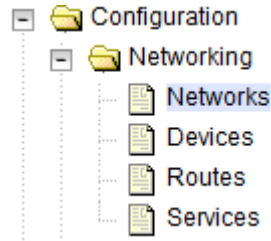
---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

4. Verify the network configuration data.
5. Expand the **Configuration** option, click **Networking** and select **Network**.

**Figure 4-2 Navigation to Networks**



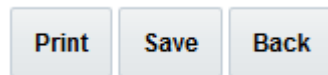
6. Click **Report**.

**Figure 4-3 Report**



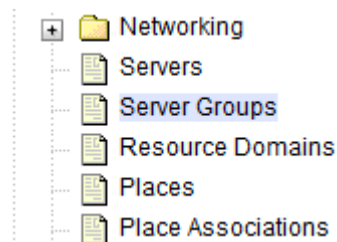
7. Verify if the configuration data is correct for your network. **Save** or **Print** this report to keep copies for future reference.

**Figure 4-4 Save or Print**



8. Verify the server configuration. Expand the **Configuration** and click the **Server Groups** option.

**Figure 4-5 Server Groups**



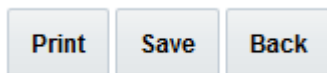
9. Click **Report**.

**Figure 4-6 Report**



10. Verify if the configuration data is correct for your network. **Save** or **Print** this report to keep copies for future reference.

**Figure 4-7 Save or Print**



11. Analyze and plan the DA-MP re-start 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 from Step 5 to 10. 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.

If this procedure fails, contact [My Oracle Support](#) for assistance.

## 4.2 Perform Health Check

### Procedure 2: Perform Health Check (Feature Activation Preparation)

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

Log in to the NOAM VIP GUI, establish a GUI session on the NOAM server by using the VIP address of the NOAM server.

1. Open the web browser and enter the URL, `http://<Primary_NOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

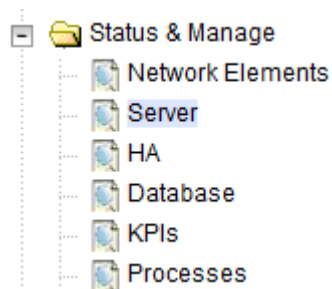
Figure 4-8 Oracle System Login



Verify the server status.

3. Expand **Status & Manage** option and click **Server**.

Figure 4-9 Server



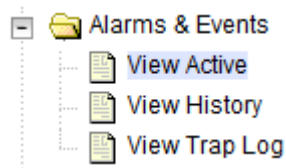
4. Verify if Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).

**Figure 4-10 Server Status**

Appl State	Alm	DB	Reporting Status	Proc
Enabled	<u>Norm</u>	Norm	Norm	<u>Norm</u>
Enabled	<u>Norm</u>	Norm	Norm	Norm
Enabled	Norm	<u>Norm</u>	Norm	Norm
Enabled	Norm	Norm	Norm	<u>Norm</u>

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 prior to 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.

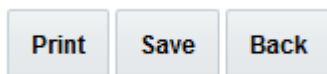
5. Log current alarms, Expand **Alarms & Events** option and click **View Active**.

**Figure 4-11 Alarms and Events**

6. Click **Report**.

**Figure 4-12 Report**

7. **Save** or **Print** this report to keep copies for future reference.

**Figure 4-13 Save or Print**

If this procedure fails, contact [My Oracle Support](#) for assistance.

# 5

## Feature Activation

Before feature activation, perform the system health check as mentioned in previous section. 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 Health Check for Pre-activation

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 [Perform Health Check](#) when preparing for feature activation, but it is repeated here to emphasize that it is being re-executed if Section [Perform Health Check](#) was performed outside the maintenance window.

### Procedure 3 : Perform Health Check (Pre Feature Activation)

Log in to the NOAM VIP GUI, establish a GUI session on the NOAM server by using the VIP address of the NOAM server.

1. Open the web browser and enter the URL, `http://<Primary_NOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

**Figure 5-1 Oracle System Login**



**ORACLE**<sup>®</sup>

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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

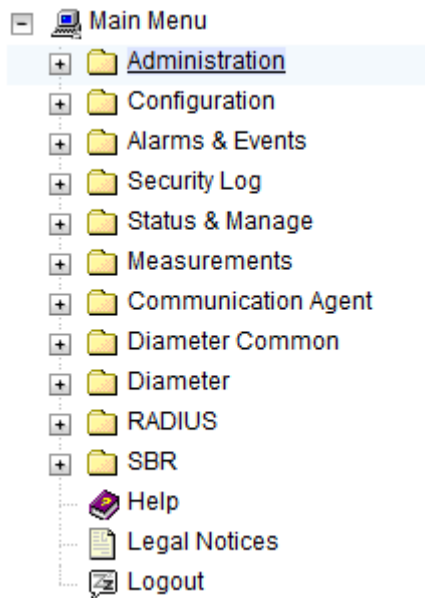
Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.  
Other names may be trademarks of their respective owners.

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Under **Main Menu**, verify the Policy and Charging folder is NOT present.



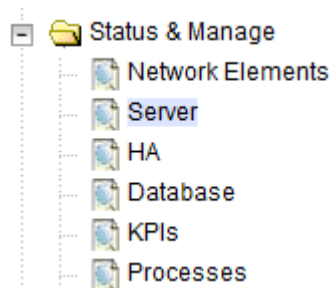
**Figure 5-2 Main Menu**



Verify the server status.

4. Expand **Status & Manage** option and click **Server**.

**Figure 5-3 Server**



5. Verify if Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).

**Figure 5-4 Server Status**

Appl State	Alm	DB	Reporting Status	Proc
Enabled	<u>Norm</u>	Norm	Norm	<u>Norm</u>
Enabled	<u>Norm</u>	Norm	Norm	Norm
Enabled	Norm	<u>Norm</u>	Norm	Norm
Enabled	Norm	Norm	Norm	<u>Norm</u>

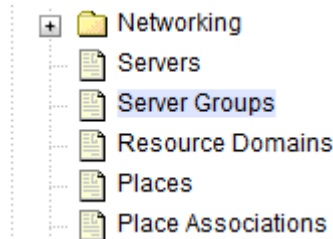
Do not proceed to feature activation if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation. If the Alarm (Alm) status is not Norm

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 prior to 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.

Verify the server configuration.

6. Expand **Configuration** option and click **Server Groups**.

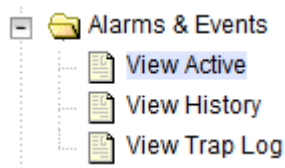
**Figure 5-5 Server Groups**



Verify the configuration data is correct for your network.

7. Log current alarms, Expand **Alarms & Events** option and click **View Active**.

**Figure 5-6 Alarms and Events**



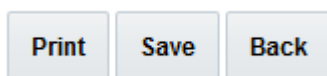
8. Click **Report**.

**Figure 5-7 Report**



9. **Save** or **Print** this report to keep copies for future reference.

**Figure 5-8 Save or Print**



Check the software version on all servers.

10. Navigate to **Administration** option, click **Software Management** and then click **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.

**Figure 5-9 Upgrade ISO Column**

DSR_DR_NO_SG   <b>DSR_NO_SG</b>   DSR_SO_SG					
Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
DSR-NO2	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0-80.18.1
	Norm	N/A	NO_SetupA		
DSR-NO-1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0-80.18.1
	Norm	N/A	NO_SetupA		

Check the Upgrade Acceptance status on all servers.

11. Navigate to **Administration** option, click **Software Management** and then click **Upgrade**.

Verify the Upgrade State column does not show **ACCEPT** or **REJECT**

 **Note:**

Upgrade must be accepted on all servers before activating PCA.

**Figure 5-10 Upgrade State Column**

DSR_DR_NO_SG   <b>DSR_NO_SG</b>   DSR_SO_SG					
Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
	Server Status	Appl HA Role	Network Element		Upgrade ISO
DSR-NO2	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0-80.18.1
	Norm	N/A	NO_SetupA		
DSR-NO-1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0-80.18.1
	Norm	N/A	NO_SetupA		

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.

If this procedure fails, contact [My Oracle Support](#) for assistance.

## 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:**
  1. For Feature Activation, see [Feature Activation](#)
  2. For Restart Process, see [Restart Process](#)
  3. For System Health Check After Application Activation on NOAM Server, see [System Health Check After Application Activation on NOAM Servers](#)
  4. For System Health Check After Application Activation on SOAM Servers, see [System Health Check After Application Activation on SOAM Servers](#)
- **For PCA activation on a newly added site:**
  1. For PCA Activation on a Newly Added Site, see [PCA Activation on a Newly Added Site](#)
  2. For Restart Process, see [Restart Process](#)
  3. For System Health Check After Application Activation on NOAM Server, see [System Health Check After Application Activation on NOAM Servers](#)
  4. For System Health Check After Application Activation on SOAM Servers, see [System Health Check After Application Activation on SOAM Servers](#)

### 5.2.1 Feature Activation

This procedure activates the PCA on complete system and does not require a Maintenance window.

1. 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. Change to the following directory:

```
$ cd /usr/TKLC/dsr/prod/maint/loaders/activate
```

3. Run the PCA application 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 [PCA Deactivation Procedure](#) to restore the system back to state before start of activation.

4. 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.**

1. Before continuing, verify all SOAM servers should be configured in the topology for the newly added site.
  - a. Log into the NOAM VIP GUI.
  - b. Expand **Status & Manage** and Click **Server**. See all required SOAM servers for the newly added site are configured and Application State is enabled.
2. For PCA activation on new site, the activation procedure needs to be executed from the NOAM. Execute the Procedures in [Feature Activation](#)

## 5.2.3 Restart Process

This procedure restarts the DSR and SBR application processes and needs to be performed in a maintenance window

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

Figure 5-11 Oracle System Login

**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

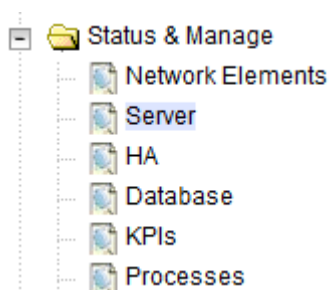
Unauthorized access is prohibited.

---

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

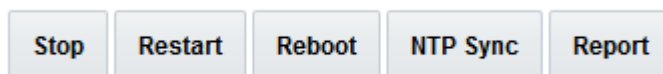
Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. 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.
4. Expand **Status & Manage** and Click **Server**.

**Figure 5-12 Server**

Select the desired DA-MPs, you can use 'Ctrl' to select multiple DA-MPs at once.

5. Click **Restart**.

**Figure 5-13 Restart**

6. 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.
7. Restart the process on SBR servers.
8. Expand **Status & Manage** and Click **Server**.
9. Select all the SBR servers, click **Restart** and **OK** to confirm

## 5.3 Post-Activation Procedures

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

### 5.3.1 System Health Check After Application Activation on NOAM Servers

This procedure verifies the PCA application activation on NOAM server and does not require a maintenance window

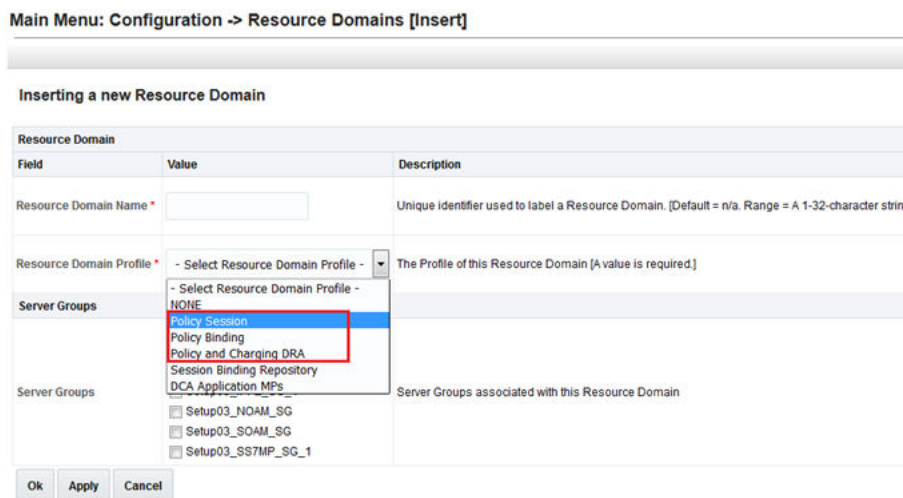
1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter the URL: `http://<Primary_NOAM_VIP_IP_Address>`
2. Login as the **guiadmin** user.

Figure 5-14 Oracle System Login



3. Verify the Resource Domain Profile shows the new profile entries.

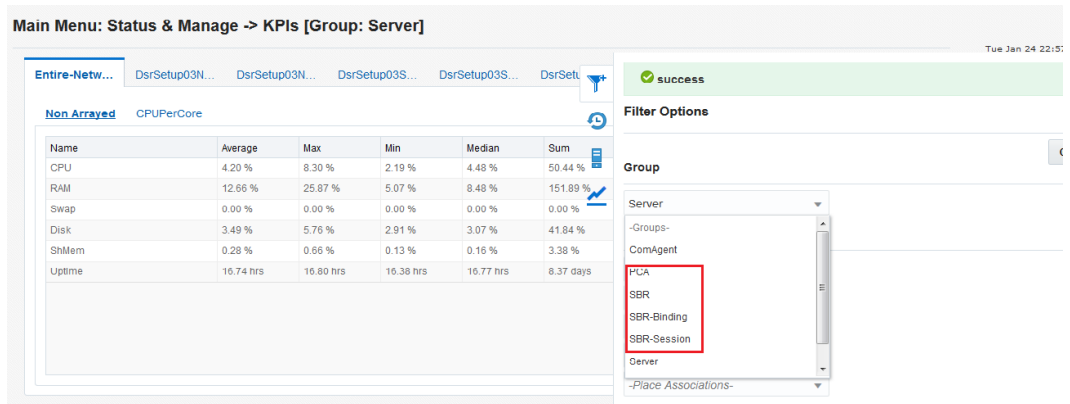
Figure 5-15 Resource Domain Profile



4. Verify KPI's filter option shows the KPI Group for PCA, SBR-Binding, and SBR-Session.

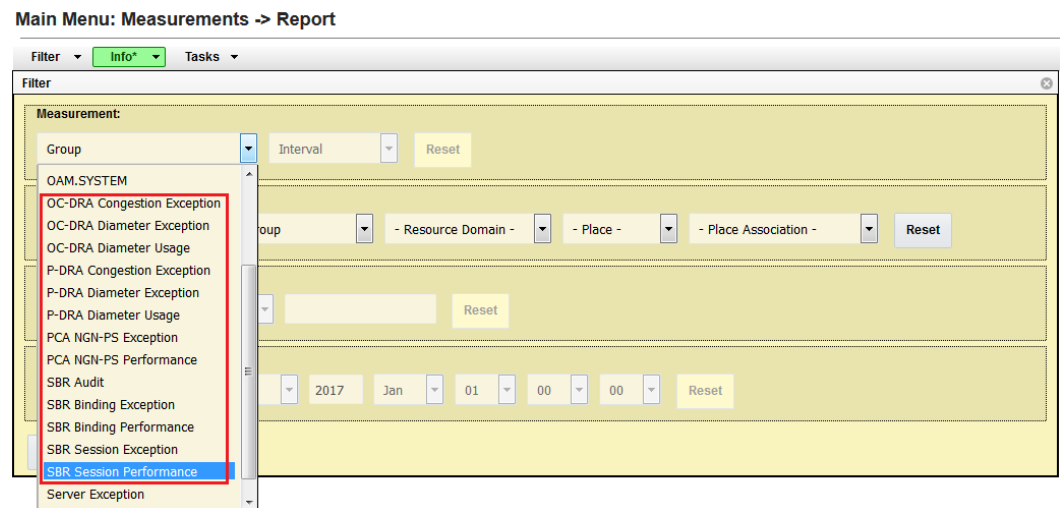


Figure 5-16 KPIs



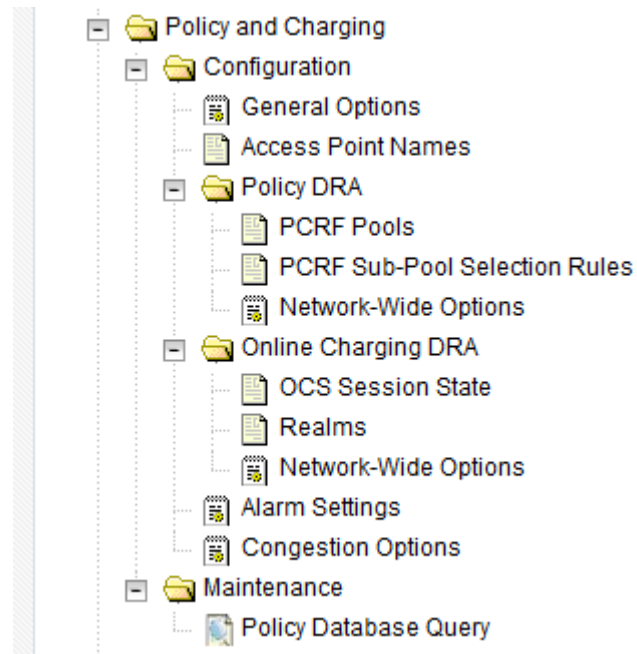
5. Verify the PCA-specific Measurement groups are shown for OC-DRA, P-DRA, and SBR.

Figure 5-17 Measurement Groups



6. Verify the **Main Menu** on active NOAM shows the Policy and Charging submenu with Configuration and Maintenance screens.

**Figure 5-18 Main Menu**



## 5.3.2 System Health Check After Application Activation on SOAM Servers

This procedure verifies the activation of PCA on SOAM servers and does not require a maintenance window.

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

Figure 5-19 Oracle System Login

**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

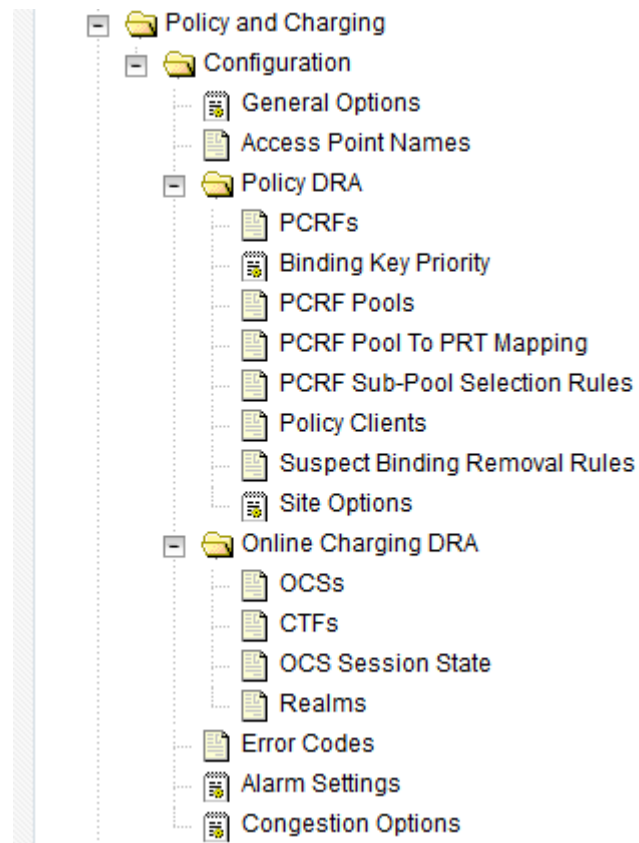
---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Verify the Policy and Charging folder appears on the left hand menu.

**Figure 5-20 Policy and Charging**



4. 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 Health Check for Pre-Deactivation

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

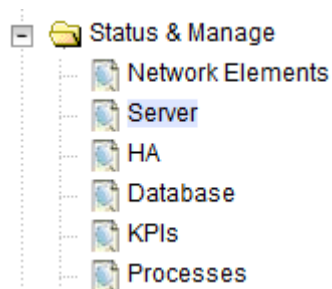
1. Log in to the NOAM VIP GUI. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter the URL `http://<Primary_NOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

**Figure 6-1 Oracle System Login**



3. Verify the server status. Expand **Status & Manage** option and click **Server**

**Figure 6-2 Server**



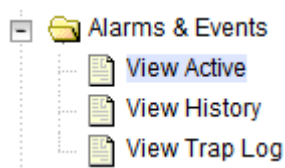
4. Verify if all Server Status is Normal (Norm) for, Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).

**Figure 6-3 Server Status**

Appl State	Alm	DB	Reporting Status	Proc
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm

5. Log the current alarms. Expand **Alarms & Events** option and click **View Active**.

**Figure 6-4 Alarms and Events**



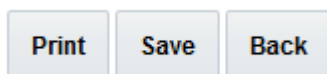
6. Click **Report**.

**Figure 6-5 Report**



7. **Save** or **Print** this report to keep copies for future reference.

**Figure 6-6 Save or Print**



Compare this alarm report with those gathered in the pre-activation procedures.  
If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.2 Deactivation Procedures

### 6.2.1 Feature Deactivation Procedure

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**
  1. For Pre PCA Deactivation Steps, see section [Pre PCA Deactivation Steps](#)
  2. For PCA Deactivation Procedure, see section [PCA Deactivation Procedure](#)
  3. For Post PCA Deactivation Steps, see section [Post PCA Deactivation Steps](#)
  4. For Post PCA Deactivation System Health Check, see section [Post PCA Deactivation System Health Check](#)
- **For PCA deactivation on a site (in the case when the site is being decommissioned)**
  1. For Site Specific PCA Deactivation Procedure, see section [Site Specific PCA Deactivation Procedure](#)

2. For Post PCA Deactivation Steps, see section [Post PCA Deactivation Steps](#)
3. For System Health Check after Application Deactivation on SOAM Servers, see section [System Health Check after Application Deactivation on SOAM Servers](#)

## 6.2.2 Pre PCA Deactivation Steps

### 6.2.2.1 Deactivate the GLA Application

This procedure deactivates the GLA application.

1. 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 the URL `http://<Primary_SOAM_VIP_IP_Address>`.
2. Log in as the `guiadmin` user.

Figure 6-7 Oracle System Login



**ORACLE**<sup>®</sup>

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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Navigate to the Applications screen. Expand **Diameter** option, click **Maintenance** and then click **Applications**.
4. 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.



- Repeat Step 1-4 on those active SOAM servers on which PCA is activated.  
If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.2.2.2 Unconfigure PCA Functions

This procedure unconfigures the PCA functions – Policy DRA and Online Charging DRA.

### 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.

- Log in to the NOAM VIP GUI. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter the URL `http://<Primary_NOAM_VIP_IP_Address>`
- Log in as the `guiadmin` user.

**Figure 6-8 Oracle System Login**



**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Navigate to **Policy and Charging** , click **Configuration** and then click **General Options**. If Policy DRA is enabled, execute the steps in reference [2], Section 4.7, to unconfigure Policy DRA.
4. Navigate to **Policy and Charging** , click **Configuration** and then click **General Options**. If Online Charging DRA is enabled, execute the steps in reference [2], Section 4.8, to unconfigure Online Charging DRA.

If this procedure fails, contact [My Oracle Support](#) for assistance.

### 6.2.2.3 Disable Diameter Connections

This procedure disables the Diameter connections.

This procedure does not require a maintenance window.



**Note:**

Repeat this procedure for all the sites on which PCA deactivation is required.

1. Log in to the SOAM VIP GUI. Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter the URL `http://<Primary_SOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

Figure 6-9 Oracle System Login

**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

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

*Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.*

3. Navigate **Diameter**, click **Maintenance** and click **Connections**.

Select all the PCA-specific diameter connections and click **Disable** or click **Disable All** (if applicable). The Admin State of connections should display as Disabled.

Figure 6-10 Connections

Main Menu: Diameter -> Maintenance -> Connections Tue Jan 24 23:49:17 2017

Filter\* Info\* Tasks

Table Description: Connections Table

Connection Name	MP Server Hostname	Dynamic	Admin State	Connection Type	Connection Mode	Operational Status	CPL	Operational Reason	Local Node	Local Port	IPFE Initiator DAMP
conn_af1	DsrSetup03 Damp1	NO	Disabled	Diameter	Responder Only	Unavailable	99	Disabled	PDRA	---	---
conn_dpi1	DsrSetup03 Damp1	NO	Disabled	Diameter	Responder Only	Unavailable	99	Disabled	PDRA	---	---
conn_pcef1	DsrSetup03 Damp1	NO	Disabled	Diameter	Responder Only	Unavailable	99	Disabled	PDRA	---	---

**Note:**

PCA-specific connection includes connections to PCRFs, PCEFs, AFs, CTFs, and OCSes.

4. Repeat Steps 1 to 3 on all active SOAM servers on which PCA deactivation is required.

If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.2.2.4 Disable Application

This procedure disables the PCA application.

This procedure does not require a maintenance window

 **Note:**

Repeat this procedure for all the sites on which PCA deactivation is required.

1. Log in to the SOAM VIP GUI. Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter the URL `http://<Primary_SOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

**Figure 6-11 Oracle System Login**

Oracle Software Web Browser Support Policy for details.' Below that is the text 'Unauthorized access is prohibited.' At the bottom, there is a horizontal line, followed by the text: 'Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.' and 'Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.'" data-bbox="270 475 820 866"/>

3. Navigate **Diameter**, click **Maintenance** and click **Applications**.

4. 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**.
5. Navigate **Diameter**, click **Maintenance** and click **Applications**. Verify the Application status has changed to **Disabled**.

**Figure 6-12 Application Table**

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

6. Repeat Steps 1 to 5 on all active SOAM servers on which PCA deactivation is required. If this procedure fails, contact [My Oracle Support](#) for assistance.

### 6.2.2.5 Remove DSR Configuration Data

This procedure removes the DSR configuration data.

#### 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. Log in to the SOAM VIP GUI. Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter the URL `http://<Primary_SOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

Figure 6-13 Oracle System Login

**ORACLE**<sup>®</sup>

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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Navigate **Diameter**, click **Configuration** and click **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**.
4. Navigate **Diameter**, click **Configuration** and click **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**.
5. Navigate **Diameter**, click **Configuration** and click **Route Lists**.  
Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
6. Navigate **Diameter**, click **Configuration** and click **Route Groups**.  
Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.
7. Navigate **Diameter**, click **Configuration** and click **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.
8. Navigate **Diameter**, click **Configuration** and click **Peer Nodes**.

Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.

9. Navigate **Diameter**, click **Configuration** and click **Local Nodes**.

Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.

10. Navigate **Diameter**, click **Configuration**, click **Configuration Sets** and then click **CEX Configuration Sets**.

Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.

11. Navigate **Diameter**, click **Configuration** and click **CEX Parameters**.

Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.

12. Navigate **Diameter**, click **Configuration** and click **Application IDs**.

Select and delete the PCA-specific or the complete configuration data (as applicable) from this screen.

13. Repeat Steps 1 to 12 on all active SOAM servers.

If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.2.2.6 Remove Resource Domain Configuration Data

This procedure removes the Resource Domain configuration data.

1. Establish a GUI session on the NOAM by using the XMI VIP address. Login as the `guiadmin` user.
2. Navigate **Configuration** and click **Resource Domains**.

Delete the Resource Domain of type 'Policy Binding' and 'Policy Session' and 'Policy and Charging DRA' from this screen.

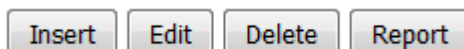
If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.2.2.7 Remove Place Associations Configuration Data

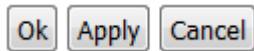
This procedure removes the Place Association configuration data.

1. Establish a GUI session on the NOAM by using the XMI VIP address. Login as the `guiadmin` user.
2. Navigate **Configuration** and click **Place Associations**.  
Select the Place Associations of type **Policy and Charging Mated Sites**.  
Click **Edit**.

**Figure 6-14** Edit



Uncheck all the Places associated with this Place Associations and click **OK**.

**Figure 6-15** Ok

Repeat this step for all other Place Associations of type **Policy and Charging Mated Sites** and **Policy Binding Region** from this screen.

3. Navigate **Configuration** and click **Place Associations**.

Delete the Place Associations of type **Policy and Charging Mated Sites** and **Policy Binding Region** from this screen.

If this procedure fails, contact [My Oracle Support](#) for assistance.

### 6.2.2.8 Remove Place Configuration Data

This procedure removes the Place configuration data. Skip this step if places are being used by DCA application.

1. Establish a GUI session on the NOAM by using the XMI VIP address. Login as the `guiadmin` user.
2. Navigate **Configuration** and click **Places**.

Edit the Places and remove servers from it.

If this procedure fails, contact [My Oracle Support](#) for assistance.

### 6.2.3 PCA Deactivation Procedure

This procedure deactivates the PCA application.

 **Note:**

Skip this step if PCA is to be activated on a particular site. Execute [Site Specific PCA Deactivation Procedure](#) instead.

1. Establish an SSH session to the NOAM VIP. Login as the `admusr`.
2. Change to the following directory:

```
$ cd /usr/TKLC/dsr/prod/maint/loaders/deactivate
```

3. Execute the PCA application deactivation script.

```
$ ./load.pcaDeactivationTopLevel
```

 **Note:**

This command execution will start 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. 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
```

If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.2.4 Site Specific PCA Deactivation Procedure

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

1. Establish an SSH session to the SOAM VIP. Login as the `admusr`.
2. Change to the following directory:

```
$ cd /usr/TKLC/dsr/prod/maint/loaders/deactivate
```

3. 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. 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
```

If this procedure fails, contact [My Oracle Support](#) for assistance.

## 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

This procedure puts all the MP servers in SBR Server Groups in OOS.

 **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.

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

**Figure 6-16 Oracle System Login**



**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Navigate **Configuration** and click **Server Groups**.
4. 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.

5. Navigate **Status & Manage** and click **HA**.

Edit the servers from list created in Step 3. Change the value of **Max Allowed HA Role** to OOS.

If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.2.5.2 Remove SBR Servers from Server Groups

This procedure removes all the MP servers in SBR Server Groups from their respective Server Groups.

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

**Figure 6-17 Oracle System Login**



**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Navigate **Configuration** and click **Server Groups**.
4. 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.

5. Navigate **Configuration** and click **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.

If this procedure fails, contact [My Oracle Support](#) for assistance.

### 6.2.5.3 Delete Server Groups related to SBR

This procedure removes the server groups related to SBR.

**Prerequisite** : Previous procedure has been executed.

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

**Figure 6-18 Oracle System Login**



**ORACLE**<sup>®</sup>

**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.  
Other names may be trademarks of their respective owners.  
Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Navigate **Configuration** and click **Server Groups**.
4. Remove the Server Groups, which has Function value **SBR**.  
If this procedure fails, contact [My Oracle Support](#) for assistance.

## 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.

### 6.2.5.4.1 Reboot the SBR Servers

This procedure removes the merge data from servers by rebooting them.



#### Note:

Select SBR servers being used for PCA application and for which deactivation has been done. Skip SBR servers being used for DCA application.

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

Figure 6-19 Oracle System Login



**ORACLE**<sup>®</sup>

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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

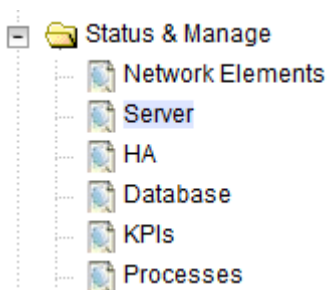
---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

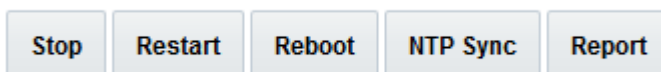
3. Navigate **Status & Manage** and click **Server**.

Figure 6-20 Server



4. Reboots all the relevant SBR servers.  
Select all the MP servers having Function “SBR” which were being used for PCA application and click **Reboot**.

Figure 6-21 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.

If this procedure fails, contact [My Oracle Support](#) for assistance.

#### 6.2.5.4.2 Reboot DA-MP Servers

This procedure removes the merge data from servers by rebooting them.

 **Note:**

Select DA-MP servers being used for PCA application and for which deactivation has been done.

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

Figure 6-22 Oracle System Login



**ORACLE**<sup>®</sup>

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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

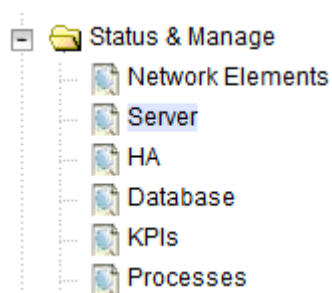
---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

3. Navigate **Status & Manage** and click **Server**.

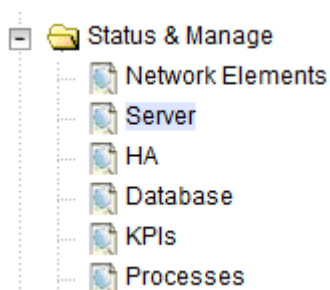
Figure 6-23 Server



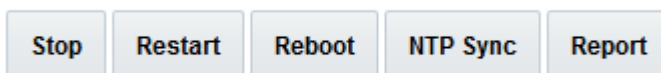
4. Multiple iterations of this step may be executed during the feature activation procedure. This is dependent on the number of DA-MP servers within your system. Make a written record of the number of times the step was performed. It is recommended that no more than 50% of the DA-MPs be restarted at once.

Navigate **Status & Manage** and click **Server**.



**Figure 6-24 Server**

Select DA-MP servers running PCA. Press **Ctrl** to select multiple DA-MPs at once. Click **Reboot**.

**Figure 6-25 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.

If this procedure fails, contact [My Oracle Support](#) for assistance.

### 6.2.5.4.3 Reboot SOAM Servers

This procedure removes the merge data from servers by rebooting them.

 **Note:**

Select SOAM servers belonging to the sites running PCA.

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

Figure 6-26 Oracle System Login

**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

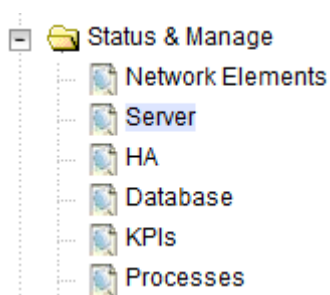
---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

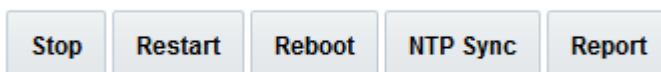
3. Navigate **Status & Manage** and click **Server**.

Figure 6-27 Server



4. Reboots all the relevant SOAM servers. Select all the SOAM servers belonging to sites running PCA and click **Reboot**.

Figure 6-28 Reboot



Verify the server changes to the Err state and wait until it returns to the Enabled/Normal state.

If this procedure fails, contact [My Oracle Support](#) for assistance.

#### 6.2.5.4.4 Reboot NOAM Servers

This procedure removes the merge data from servers by rebooting them.

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

**Figure 6-29 Oracle System Login**



**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

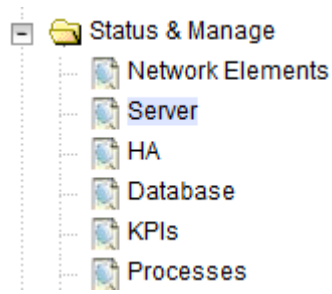
---

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

Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.

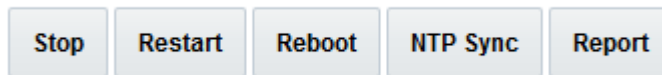
3. Navigate **Status & Manage** and click **Server**.

**Figure 6-30 Server**



4. Select all NOAM servers except the active NOAM and click **Reboot**.

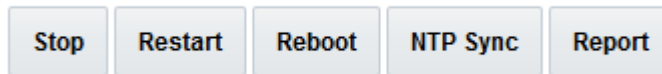
**Figure 6-31 Reboot**



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**.

**Figure 6-32 Reboot**



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.

If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.2.6 Post PCA Deactivation System Health Check

### 6.2.6.1 System Health Check after PCA Deactivation on NOAM Server

This procedure verifies the PCA application deactivation on NOAM server.

 **Note:**

Execute this procedure only when PCA is deactivated on entire network. If PCA is deactivated on a particular site, skip this procedure.

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

Figure 6-33 Oracle System Login

**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

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

---

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

*Copyright © 2010, 2016, [Oracle](#) and/or its affiliates. All rights reserved.*

3. Verify the Resource Domain Profile list does not show the profile entries of **Policy and Charging DRA, Policy Session, and Policy Binding**.

Figure 6-34 New Resource Domain

Main Menu: Configuration -> Resource Domains [Insert] Tue

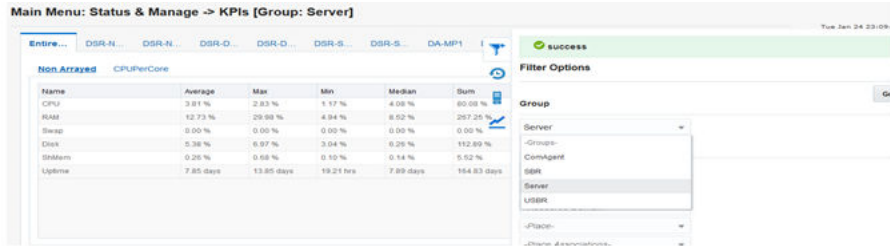
---

Inserting a new Resource Domain

Field	Value	Description
Resource Domain Name *	<input type="text"/>	Unique identifier used to label a Resource Domain. [Default = n/a. Range = A 1-32-character string. Valid characters are alphanumeric and underscore.]
Resource Domain Profile *	- Select Resource Domain Profile -	The Profile of this Resource Domain [A value is required.]
Server Groups	<input type="text"/> <ul style="list-style-type: none"> <li>- Select Resource Domain Profile -</li> <li>Subject Resource Domain Profile -</li> <li>NONE</li> <li>Session Binding Repository</li> <li>DCA Application MPs</li> <li>ITSR TOR N1Y SG</li> </ul>	

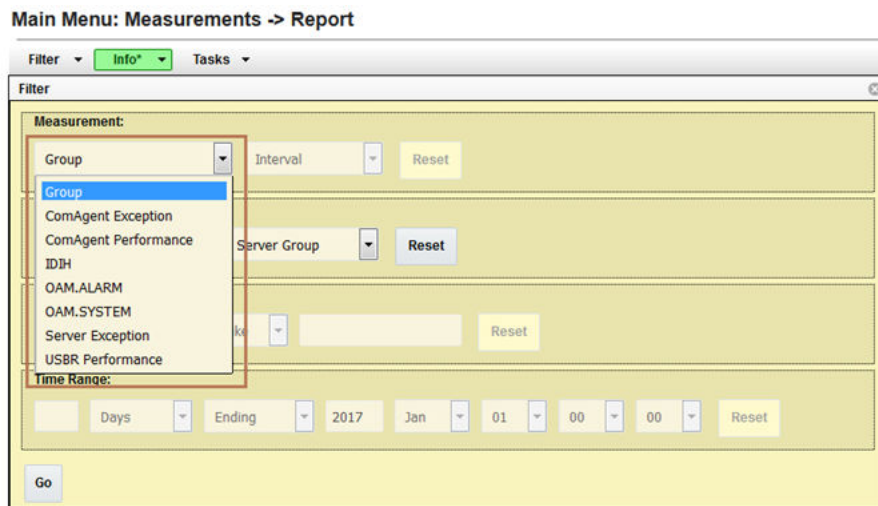
4. Verify KPIs filter option do not show the KPI groups for PCA, SBR-Binding and SBR-Session.

**Figure 6-35 KPI**

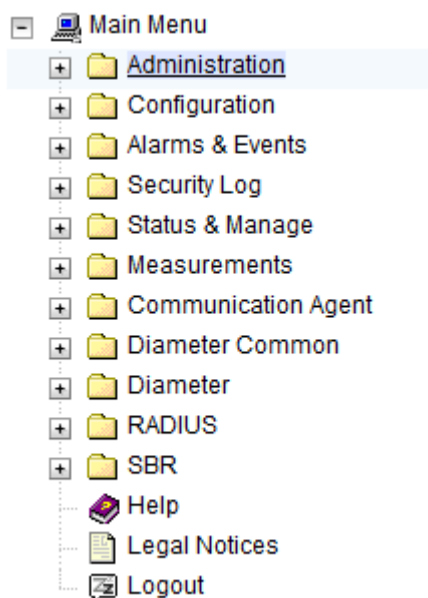


5. Verify Measurement groups are not shown for OC-DRA, P-DRA, SBR-Binding, and SBR-Session.

**Figure 6-36 Measurement**



6. Verify Main Menu on active NOAM does not show the Policy and Charging submenu.

**Figure 6-37 Main menu**

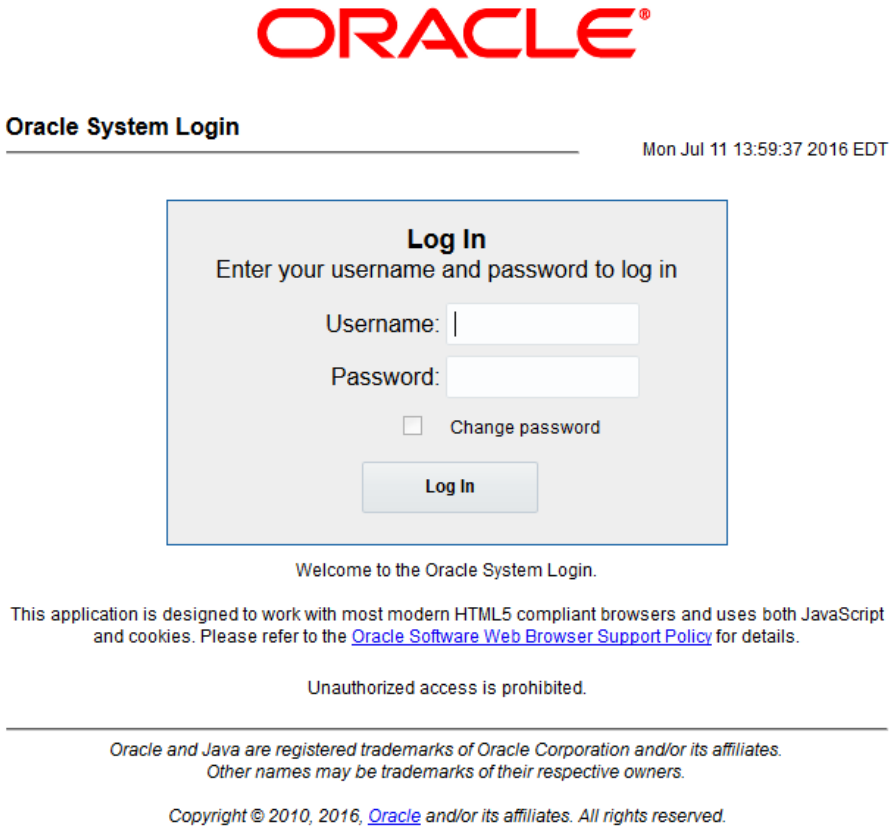
If this procedure fails, contact [My Oracle Support](#) for assistance.

### 6.2.6.2 System Health Check after Application Deactivation on SOAM Servers

This procedure verifies the PCA application deactivation on SOAM servers.

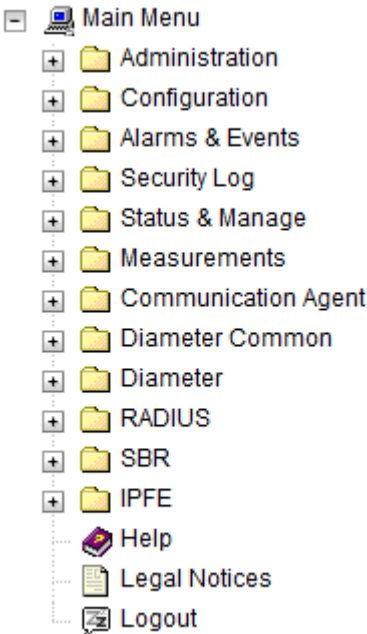
1. Log in to the SOAM VIP GUI. Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter the URL `http://<Primary_SOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

Figure 6-38 Oracle System Login



- 3. Verify the Policy and Charging folder does not appear on the left hand menu:

Figure 6-39 Main menu





4. Verify the Diameter maintenance application menu do not show the entry of PCA application.

**Figure 6-40 Application Menu**

Main Menu: Diameter -> Maintenance -> Applications

Filter\* ▼

Table Description: Applications Table

Application Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Congestion Level	Time of Last Update
------------------	--------------------	-------------	--------------------	--------------------	------------------	---------------------

5. Repeat Steps 1 to 4 on all active SOAM servers for which PCA has been deactivated. If this procedure fails, contact [My Oracle Support](#) for assistance.

## 6.3 Post-Deactivation Procedures

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

### 6.3.1 Health Check for Post-Feature Deactivation

This procedure performs a post activation health check.

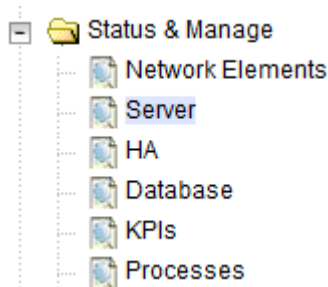
1. Log in to the NOAM VIP GUI. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter the URL `http://<Primary_NOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

**Figure 6-41 Oracle System Login**



3. Navigate **Status & Manage** and click **Server**.

**Figure 6-42 Server**



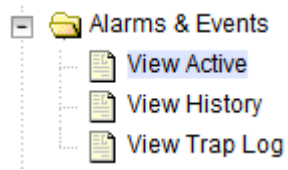
Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Reporting Status, and Processes (Proc).

**Figure 6-43 Server status**

Appl State	Alm	DB	Reporting Status	Proc
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm

4. Navigate **Alarms & Events** and click **View Active**.

**Figure 6-44 Alarms and Events**



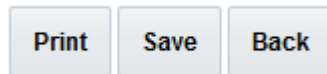
5. Click **Report**.

**Figure 6-45 Report**



6. **Save** or **Print** this report to keep copies for future reference.

**Figure 6-46 Save or Print**



Compare this alarm report with those gathered in the pre-Deactivation procedures.  
If this procedure fails, contact [My Oracle Support](#) for assistance.

# 7

## Engineering Notes

**FIPS integrity verification test failed:** In DSR 7.1 and later, 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.pcaActivateAsScoped
script on DsrSetup03Noam1
===== Start of Log Data in file /var/TKLC/log/pcaActivateAsScoped.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=YesshutdownMode=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 ===
=====E-N-
D=====
Execution status of activation script on DsrSetup03Noam1: PASSED
Please check /var/TKLC/log/pcaActivateAsScoped.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.pcaActivateStandByAsScoped script on DsrSetup03Noam2
FIPS integrity verification test failed.
===== Start of Log Data in file /var/TKLC/log/
pcaActivateStandbyAsScoped.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.pcaDeactivateStandByAsscoped script on DsrSetup03Noam2
FIPS integrity verification test failed.
===== S-T-A-R-T of log pcaDeactivateAsscoped.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/pcaDeactivateAsscoped.log.DsrSetup03Noam2
for more details.
FIPS integrity verification test failed.
```

FIPS integrity verification test failed.  
pcaDeactivateAsScoped.log

100% 963 0.9KB/s 00:00

Starting Deactivation on Active NOAMP server.

Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/  
load.pcaDeactivateAsScoped script on DsrSetup03Noam1  
===== Start of Log Data in file /var/TKLC/log/pcaDeactivateAsScoped.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 ===

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]$
```

# 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.

# A

## PCA Activation on Active NOAM

This procedure activates the PCA on a NOAM system.

This procedure does not require a Maintenance window.

1. 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. Change to the following directory:

```
$ cd /usr/TKLC/dsr/prod/maint/loaders/activate
```

3. 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 [PCA Deactivation Procedure](#) to restore the system back to state before start of activation.

4. Delete all GUI cache files on active NOAM for quick view of changes or wait for some time so new changes are reflected.

```
$ clearCache
```

If this procedure fails, contact [My Oracle Support](#) for assistance.

### Sample Output of Activation for 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 ===
=====E-N-
D=====

```

# B

## PCA Activation on Standby NOAM

This procedure activates the PCA on a NOAM system.

This procedure does not require a Maintenance window.

1. 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>
```

2. Change to the following directory:

```
$ cd /usr/TKLC/dsr/prod/maint/loaders/activate
```

3. Run the feature activation script by executing the following command:

```
$ ./load.pcaActivateStandByAscped
```

 **Note:**

This command execution starts activation on NOAM servers and All Active SOAM servers.

Check the `/var/TKLC/log/pcaActivateStandbyAscped.log` file to see if there is any execution failure.

If the activation fails, then execute the procedure in Section [PCA Deactivation Procedure](#) to restore the system back to state before start of activation.

4. Delete all GUI cache files on active NOAM for quick view of changes or wait for some time so new changes are reflected.

```
$ clearCache
```

If this procedure fails, contact [My Oracle Support](#) for assistance.



**Sample Output of Activation for 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=6name=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=====
=====
==
```

# C

## PCA Activation on Active SOAM

This procedure activates the PCA on a SOAM system.

This procedure does not require a Maintenance window.

1. 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. Change to the following directory:

```
$ cd /usr/TKLC/dsr/prod/maint/loaders/activate
```

3. 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 [PCA Deactivation Procedure](#) to restore the system back to state before start of activation.

4. Delete all GUI cache files on active SOAM for quick view of changes or wait for some time so new changes are reflected.

```
$ clearCache
```

If this procedure fails, contact [My Oracle Support](#) for assistance.

### Sample Output of Activation for Active SOAM:

```
[admusr@S01 activate]$ ./load.pcaActivateBscoped
===== Start of Log Data in file /var/TKLC/log/pcaActivateBscoped.log
=====
Server Name : S01
Server Role: SYSTEM_OAM
Node Id    : S01
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=====
=====
==

```

# D

## PCA Activation on Standby SOAM

This procedure activates the PCA on a SOAM system.

This procedure does not require a Maintenance window.

1. Establish a secure shell session on the standby 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. Change to the following directory:

```
$ cd /usr/TKLC/dsr/prod/maint/loaders/activate
```

3. 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 [PCA Deactivation Procedure](#) to restore the system back to state before start of activation.

4. Delete all GUI cache files on active SOAM for quick view of changes or wait for some time so new changes are reflected.

```
$ clearCache
```

If this procedure fails, contact [My Oracle Support](#) for assistance.

### Sample Output of Activation for 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@S02 activate]#