Oracle® Database

Diameter Signaling Router Diameter Custom Applications Feature Activation Guide

Release 9.3.0.0.0
G56059-01
May 2026

ORACLE

Oracle Database Diameter Signaling Router Diameter Custom Applications Feature Activation Guide, Release 9.3.0.0.0

G56059-01

Contents

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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.

What's New in This Guide

This section introduces the documentation updates for Release 9.3.0.0.0.

Release 9.3.0.0.0 - G56059-01, May 2026

There are no updates in this release.

Acronyms and Terminology

An alphabetized list of acronyms used in the document is listed below:

Table Acronyms and Terminology

Acronym	Definition
BNS	Broadband Networking Solutions
DCA	Diameter Custom Applications
CAPM	Computer-Aided Policy Making
DA-MP	Diameter Agent Message Processor
DB	Database
DSR	Diameter Signaling Router
FOA	First Office Application
GUI	Graphical User Interface
HA	High Availability
IMI	Internal Management Interface
IP	Internet Protocol
MP	Message Processing or Message Processor
NE	Network Element
NO	Network OAM
NOAM	Network OAM
OAM	Operations, Administration and Maintenance
SSH	Secure Shell
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface
NOAM	Network Operations and Maintenance
SOAM	System Operations and Maintenance

1 Introduction

This document describes the procedure executed to activate the Diameter Custom Applications (DCA) feature (or beyond) Network Element (NE).

This procedure may be executed in either of the following scenarios:

- As part of a new DSR installation, after the standard installation is complete but before the NE is in service.
- On an DSR NE in-service, where the DCA feature is activated during a planned maintenance window to minimize the impact on network traffic.

This document also provides a procedure to deactivate the DCA framework and applications after it has been activated. Refer to the Feature De-Activation section for the deactivation procedures.

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

2

Feature Activation Overview

This section describes the procedures for activating the DCA feature. In addition, the information tabulated in the following tables provide estimates of the time required to execute the procedure:

1. Table 4-1
2. Table 5-1
3. Table 5-2
4. Table 6-1
5. Table 7-1
6. Table 8-1
7. Table 8-2
8. Table 9-1

These tables can be used to estimate the total time necessary to complete the feature activation. The timing values depicted are only estimates. Use the above tables to plan the timing of the activation and not for the execution of the procedure.

The detailed procedure steps to be executed are described in Feature Activation Preparation.

3 Definition of Activation for the DCA Feature

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

All the software required to run Diameter Custom Applications is available by default as part of a DSR installation or upgrade package. The process of activating the feature simply makes proper use of software elements and file system files that are already present to change the behavior of the DSR NE.

Table 3-1 Behavior of DCA Framework and Application Activation and Deactivation

Sl No.	DCA	Behavior
1.	DCA Framework Activation	DCA Framework Activation
2.	DCA Application Activation	DCA Application Activation
3.	DCA Application Deactivation	DCA Application Deactivation
4.	DCA Framework Deactivation	DCA Framework Deactivation

4 Pre-Feature Activation Overview

The pre-activation procedures provided in the following table can be executed outside a maintenance window (optional). Procedure completion time displayed here are estimates. The actual time taken may vary due to differences in database size, network configuration and loading, user experience, and user preparation.

Table 4-1 Pre-Feature Activation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation
	This Step	Cum.	
System Topology Check	0:10-0:30	0:20-1:00	• Verify network element configuration data. • Verify the system group configuration data.
Perform Health Check	0:01-0:05	0:21-1:05	• Verify DSR release. • Verify server status. • Log all current alarms.

5

Feature Activation Execution Overview

The procedures shown in the following table are executed within a single 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 5-1 DCA Framework Activation Execution Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation	Impact
	This Step	Cum.		
Perform Health Check - Pre-Feature Activation	0:01-0:05	0:01-0:05	• Verify DSR release. • Verify proper DCA feature state. • Verify server status. • Log all current alarms.	None.
DCA Framework Activation	0:10-0:30	0:11-0:35	• Log out of NOAM GUI. • SSH to active NO. • Change to the feature activation directory. • Execute the feature activation script. • Log into active NOAM and SOAM GUI. • Verify the DCA framework folder. • Close SSH connections to both NOAM.	DCA framework is activated on DSR.

The procedures shown in the following table are executed inside a single 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 5-2 DCA Application Activation Execution Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation	Impact
	This Step	Cum.		
DCA Application Activation	0:10-0:30	0:11-0:35	• Log out of NOAM GUI. • SSH to active NO. • Change to the feature activation directory. • Execute the feature activation script. • Log into active NOAM and SOAM GUI. • Verify the DCA application folder. • Close SSH connections to both NOAMs.	DCA application is activated on DSR.

6
Post-Feature Activation Overview

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

Table 6-1 Post-Feature Activation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation	Impact
	This Step	Cum.		
Perform Health Check Post-Feature Activation	0:01-0:05	0:01-0:05	• Verify Server status. • Log all current alarms.	DCA has been activated on DSR.

7

Pre-Feature Deactivation Overview

The procedures given 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 7-1 Pre-Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation	Impact
	This Step	Cum.		
Pre-Feature Deactivation Perform Health Check	0:01-0:05	0:01-0:05	• Verify the DSR release. • Verify proper DCA state. • Verify server status. • Log current alarms	None.

8

Feature Deactivation Execution Overview

The procedures given 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 8-1 DCA Application Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation	Impact
	This Step	Cum.		
Deactivation set up.	0:10-0:30	0:10-0:30	The reason to deactivate has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time varies.	None.
DCA Application Deactivation	00:10-00:20	0:20-0:50	• Log out of active NOAM GUI. • SSH into active NO. • Change directory. • Execute the feature deactivation script. • Log into active NOAM and SOAM GUI. • Verify the DCA application folder. • Close SSH connections to both NOAMs.	DCA application is deactivated on DSR.

Table 8-2 DCA Framework Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation	Impact
	This Step	Cum.		
Deactivation set up.	0:10-0:30	0:10-0:30	The reason to deactivate has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time varies.	None.
DCA Framework Deactivation	00:10-00:20	0:20-0:50	• Log out of active NOAM GUI. • SSH into active NO. • Change directory. • Execute the feature deactivation script. • Log into active NOAM and SOAM GUI. • Verify the DCA folder. • Close SSH connections to both NOAMs.	DCA framework is deactivated on the DSR.

9

Post Feature Deactivation Overview

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

Table 9-1 Post-Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation
	This Step	Cum.	
Perform Health Check Post-Feature Deactivation	0:01-0:05	0:01-0:05	• Verify server status. • Log all current alarms.

10

Feature Activation Preparation

It is expected that Oracle personnel following this Feature Activation Procedure document will activate the DCA framework first on a customer's DSR, then activate the DCA application as required for that customer.

This section provides detailed procedures for preparing a system for DCA feature activation. These procedures are executed outside a maintenance window.

10.1 System Topology Check

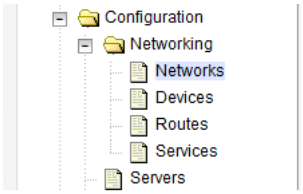
This procedure is part of feature activation preparation and is used to verify the system topology of the DSR network and servers.

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 10-1 Oracle System Log in

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

Figure 10-2 Network Folder

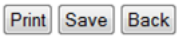


6. Click **Report**

Figure 10-3 Report

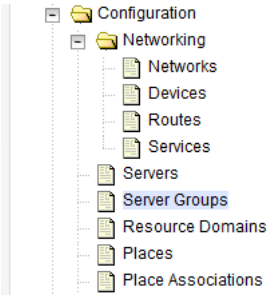
7. Verify if the configuration data is correct for your network. Click **Save** or **Print** this report to keep copies for future reference.

Figure 10-4 Save or Print



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

Figure 10-5 Server Group

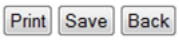


9. Click **Report**

Figure 10-6 Report

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

Figure 10-7 Save or Print



If this procedure fails, contact My Oracle Support (MOS) for assistance.

10.2 Perform Health Check

This procedure is part of feature activation preparation and is used to determine the health and status of the DSR network and servers. This can be run more than once, but it must be run at

least once within 24-36 hours of the start of the maintenance window during which the feature activation will take place.

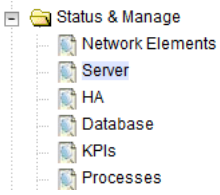
Log in to the NOAM VIP GUI and establish a GUI session on the NOAM server by using the VIP address of the NOAM server.

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

Figure 10-8 Oracle System Log in

3. Verify DSR release.
4. Expand **Administration** option and click **Software Version** to verify the Eagle XG DSR RPM version shows version 8.0.0 or greater.
5. Verify the Server Status. Expand **Status & Manage** and click **Server**.

Figure 10-9 Status and Manage



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

Figure 10-10 Alarms

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

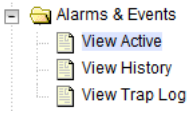
Do not proceed to feature activation if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.

If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the feature activation. If there are Major or Critical alarms present, these

alarms should be analyzed before proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms.

7. In the NOAM VIP GUI, log the current alarms. Expand the **Alarms & Events** option and click **View Active**

Figure 10-11 View Active Alarms

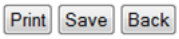


8. Click **Report**.

Figure 10-12 Report

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

Figure 10-13 Save or Print

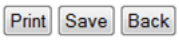


10. In the NOAM VIP GUI, log the alarm history. Expand **Alarms & Events** option and click **View History**.
11. Click **Report**

Figure 10-14 Report

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

Figure 10-15 Save or Print



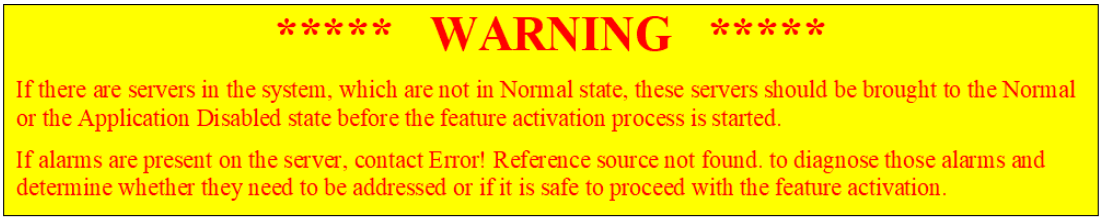
If this procedure fails, contact My Oracle Support (MOS) for assistance.

11

Feature Activation

Before feature activation, perform the system health check as described in Perform Health Check. This check ensures the system is ready for feature activation. Performing the system health check determines the alarms present in the system and helps to determine if the feature can be activated with the alarms present in the system.

Figure 11-1 Warning



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 host names.
  - 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 track each step. The technician must track each iteration of the step that is executed.
- Captured data is required for future support reference.

12
Perform Health Check - Pre-Feature Activation

This section describes the procedure to perform a health check pre-feature activation.

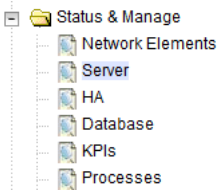
Log in to the NOAM VIP GUI and establish a GUI session on the NOAM server by using the VIP address of the NOAM server.

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

Figure 12-1 Oracle System Log in

3. In the NOAM (2-Tiered) VIP GUI, verify if the DCA Framework folder is not present. Expand the **Main Menu** option and click **Diameter**.
4. In the SOAM (2-Tiered) VIP GUI, verify if the DCA Framework folder is not present. Expand the **Main Menu** option and click **Diameter**.
5. Verify the Server Status. Expand **Status & Manage** and click on **Server**.

Figure 12-2 Status and Manage



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

Figure 12-3 Alarms

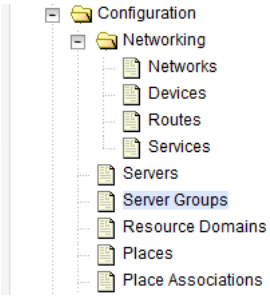
Appl State	Alm	DB	Reporting Status	Proc
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm

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

If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the feature activation. If there are Major or Critical alarms present, these alarms should be analyzed before proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms.

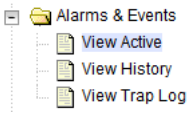
7. In the NOAM VIP GUI, verify the server configuration. Expand the **Configuration** option, and then click **Server Groups**. Verify if the configuration data is correct in the network.

Figure 12-4 Server Group



8. In the NOAM VIP GUI, log the current alarms. Expand the **Alarms & Events** option and click **View Active**.

Figure 12-5 View Active Alarms



9. Click **Report**

Figure 12-6 Report

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

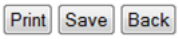
Figure 12-7 Save or Print

11. In the NOAM VIP GUI, log the alarm history. Expand **Alarms & Events** option and click **View History**.
12. Click **Report**.

Figure 12-8 Report

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

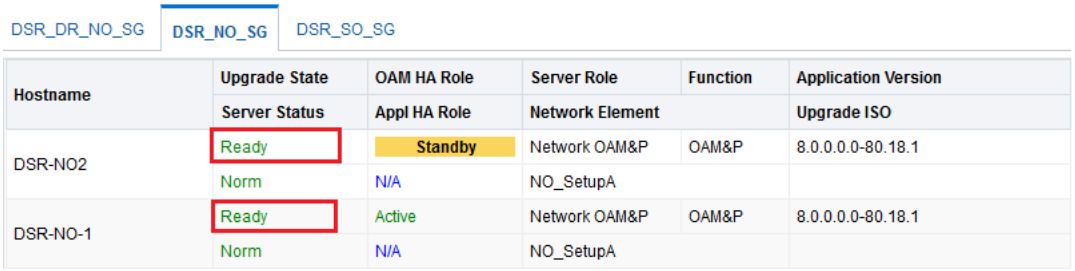
Figure 12-9 Save or Print



14. In the NOAM VIP GUI, check the Upgrade Acceptance status on all servers. Expand the **Administration** option, navigate to **Software Management**, and click **Upgrade**. Verify if the Upgrade State column does not show ACCEPT or REJECT.

> **Note**
>
> Upgrade must be accepted on all servers before activating DCA.

Figure 12-10 Upgrade



Upgrade State should be **Ready**. If the Upgrade State is **ACCEPT** or **REJECT**, follow the procedure documented in DSR C-Class Software Installation and Configuration guide or DSR Software Upgrade Guide (as applicable) to accept the upgrade on all servers before activating DCA.

If this procedure fails, contact My Oracle Support (MOS) for assistance.

13
Activation Procedures

This section provides the detailed procedure steps of the feature activation execution. These procedures are executed inside a maintenance window.

13.1 DCA Framework Activation

This procedure verifies that the feature activation steps have been completed.

1. Log out of any active NOAM VIP GUI sessions.
2. Establish a secure shell session on the active NOAM VIP GUI by using the XMI VIP address. Log in as `admusr`. Use your SSH client to connect to the server (for example, 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>
   ```

3. Change to the following directory:

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

4. Execute the DCA activation script. Run the DCA activation script by executing the following command:

   ```
   # ./featureActivateDeactivate
   ```

   Choose **Activate** and **DCA Framework** options.

   There is an option to choose to activate this feature on all SOAMs or on a specific SOAM. It is recommended to select **Activate on all SOAM**.

   > **Note**
   >
   > If a new site is added or if a SOAM site framework was not activated, the activation script can be executed again to add the application on new sites. The script does not have any impact on the sites on which the framework is already active.

   Verify the screen output is similar to Sample DCA Framework Activation.
5. Log in to the active NOAM VIP and SOAM VIP GUIs.

6. Verify the **DCA Framework** folder and the **Configuration** sub-menu.

   On NOAM VIP GUI, verify if the **DCA Framework** folder displays under the **DSR Main Menu** with **Configuration** as a sub-menu. On SOAM VIP GUI, verify if the **DCA Framework** folder displays under the **DSR Main Menu** with **Configuration** as a sub-menu.

7. Close SSH connection to active NOAM VIP GUIs. Log out of the active NOAM VIP GUI log in shell and close the SSH connections by executing the following command:

   ```
   # exit
   ```

   Close the SSH connection.

   If this procedure fails, contact My Oracle Support (MOS) for assistance.

13.2 DCA Application Activation

The DCA framework must be activated before any application can be activated.

1. Log out of any active NOAM VIP GUI sessions.
2. Establish a secure shell session on the active NOAM VIP GUI by using the XMI VIP address. Log in as `admusr`. Use your SSH client to connect to the server (for example 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>
   ```

3. Change to the DCA activation directory, execute the following command:

   ```
   # cd /usr/TKLC/dsr/prod/maint/loaders/
   ```

4. Execute the DCA activation script. Run the DCA activation script by executing the following command:

   ```
   # ./featureActivateDeactivate
   ```

   Choose **Activate** and **DCA Application** options.

   When asked, select **Activate a DCA Application**.

   > **Note**
   >
   > The above option is not asked the DCA is not active on the system. The script goes directly to **Activate a DCA Application** mode.

   When asked, **Enter the long name for the DCA application**.

> **Note**
>
> The DCA long name should consist of a combination of letters, numbers, and spaces and should not begin with a space. It has a maximum of 32 characters.

When asked, **Enter the short name for the DCA application**.

> **Note**
>
> The DCA short name should consist of a combination of letters and numbers. It has a maximum of 6 characters.

Verify the screen looks similar to the sample DCA Application Activation.

Expand the option **Status & Manage** and click **Server** to restart the DSR MP.

5. Log in to the active NOAM VIP and SOAM VIP GUIs.
6. In the NOAM VIP and SOAM VIP GUIs, verify the DCA Application folder and sub-menus.

   On the NOAM VIP GUI , verify the DCA folder with the name provided in step 4 displays under the DCA Framework menu. Sub-menus should include: General Options, Trial MP assignment, and Application Control.

   On SOAM VIP GUI, verify the DCA folder with the name provided in step 4 displays under the DCA Framework menu. Sub-menus should include: General Options, Trial MP assignment, Application Control, and System Options.
7. Close SSH connection to active NOAM VIP GUIs. Log out of the active NOAM VIP GUI log in shell and close the SSH connections by executing the following command:

   ```
   # exit
   ```
   Close the SSH connection.

   If this procedure fails, contact My Oracle Support (MOS) for assistance.

13.3 DCA Application Re-activation

DCA Feature reactivation option is executed mainly during Disaster Recovery. It allows reactivating all the activated DCA Applications in the system after Disaster Recovery procedure is executed. Detailed steps are given in the procedure below.

This procedure verifies that the global admin has been enabled.

1. Log out of any active NOAM VIP GUI sessions.
2. Establish a secure shell session on the active NOAM VIP GUI by using the XMI VIP address. Log in as `admusr`. Use your SSH client to connect to the server (for example 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>
```

3. Change to the DCA activation directory, execute the following command:

   ```
   # cd /usr/TKLC/dsr/prod/maint/loaders/
   ```

4. Execute the DCA activation script. Run the DCA activation script by executing the following command:

   ```
   # ./featureActivateDeactivate
   ```
   Choose **Activate** and **DCA Application** options.

   When asked, select **Activate a DCA Application**.

   > **Note**
   >
   > The above option is not asked the DCA is not active on the system. The script goes directly to **Activate a DCA Application** mode.

   When asked, **Enter the long name for the DCA application**.

   > **Note**
   >
   > The DCA long name should consist of a combination of letters, numbers, and spaces and should not begin with a space. It has a maximum of 32 characters.

   When asked, **Enter the short name for the DCA application**.

   > **Note**
   >
   > The DCA short name should consist of a combination of letters and numbers. It has a maximum of 6 characters.

   Verify the screen looks similar to the sample DCA Application Re-activation.

   Expand the option **Status & Manage** and click **Server** to restart the DSR MP.

5. Log in to the active NOAM VIP and SOAM VIP GUIs.

6. In the NOAM VIP and SOAM VIP GUIs, verify the DCA Application folder and sub-menus.

   On the NOAM VIP GUI , verify the DCA folder with the name provided in Step 4 displays under the DCA Framework menu. Sub-menus should include: General Options, Trial MP assignment, and Application Control.

   On SOAM VIP GUI, verify the DCA folder with the name provided in Step 4 displays under the DCA Framework menu. Sub-menus should include: General Options, Trial MP assignment, Application Control, and System Options.

7. Close SSH connection to active NOAM VIP GUIs. Log out of the active NOAM VIP GUI log in shell and close the SSH connections by executing the following command:

   ```
   # exit
   ```
   Close the SSH connection.

   If this procedure fails, contact My Oracle Support (MOS) for assistance.

13.4 Perform Health Check Post-Feature Activation

This procedure is used to determine the health and status of the DSR network and servers. This procedure performs a health check.

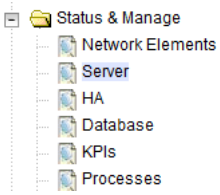
Log in to the NOAM VIP GUI, establish a GUI session on the NOAM server by using the VIP address of the NOAM server.

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

Figure 13-1 Oracle System Log in

3. Verify the Server Status. Expand **Status & Manage** click on **Server**

Figure 13-2 Status and Manage



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

Figure 13-3 Alarms

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

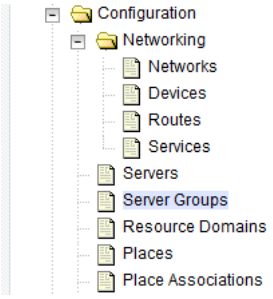
Do not proceed to feature activation if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.

If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the feature activation. If there are Major or Critical alarms present, these

alarms should be analyzed before proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms.

5. In the NOAM VIP GUI, verify the server configuration. Expand the option **Configuration** and click **Server Groups**.

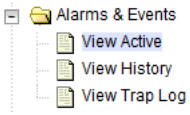
Figure 13-4 Server Groups



Verify the configuration data is correct for your network.

6. In the NOAM VIP GUI, log the current alarms. Expand the **Alarms & Events** option and click **View Active**

Figure 13-5 View Active Alarms



7. Click **Report**

Figure 13-6 Report

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

Figure 13-7 Save or Print

9. In the NOAM VIP GUI, log the alarm history. Expand **Alarms & Events** option and click **View History**.
10. Click **Report**

Figure 13-8 Report

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

Figure 13-9 Save or Print

If this procedure fails, contact My Oracle Support (MOS) for assistance.

14

Feature Deactivation

This section describes the procedures to deactivate the DCA feature.

15
Pre-deactivation Procedures

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

15.1 Pre-Feature Deactivation Perform Health Check

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

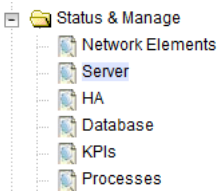
Log in to the NOAM VIP GUI and establish a GUI session on the NOAM server by using the VIP address of the NOAM server.

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

Figure 15-1 Oracle System Log in

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

Figure 15-2 Status and Manage



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

Figure 15-3 Alarms

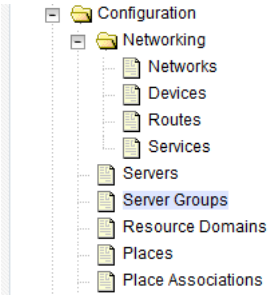
Appl State	Alm	DB	Reporting Status	Proc
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm

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

If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the feature activation. If there are Major or Critical alarms present, these alarms should be analyzed before proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms.

5. In the NOAM VIP GUI, verify the server configuration. Expand the option **Configuration** and click **Server Groups**.

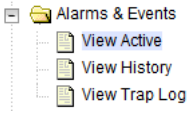
Figure 15-4 Server Groups



Verify the configuration data is correct for your network.

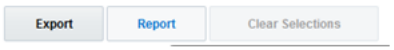
6. In the NOAM VIP GUI, log the current alarms. Expand the **Alarms & Events** option and click **View Active**

Figure 15-5 View Active Alarms



7. Click **Report**.

Figure 15-6 Report



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

Figure 15-7 Save or Print

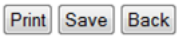
9. In the NOAM VIP GUI, log the alarm history. Expand **Alarms & Events** option and click **View History**.

10. Click **Report**

Figure 15-8 Report

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

Figure 15-9 Save or Print



If this procedure fails, contact My Oracle Support (MOS) for assistance.

16
Deactivation Procedures

This sections describe the procedures to deactivate the DCA feature.

16.1 DCA Application Deactivation

This procedure verifies that the feature deactivation steps have been completed.

1. Log out of any active NOAM VIP GUI sessions.
2. Establish a secure shell session on the active NOAM VIP GUI by using the XMI VIP address. Log in as `admusr`. Use your SSH client to connect to the server (for example, 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>
   ```

3. Change to the DCA activation directory, execute the following command:

   ```
   # cd /usr/TKLC/dsr/prod/maint/loaders/
   ```

4. Execute the DCA activation script. Run the DCA activation script by executing the following command:

   ```
   # ./featureActivateDeactivate
   ```

   Choose **Activate** and **DCA Application** options.

   When asked, select **Enter the name for the DCA application to be deactivated**.

   Verify the screen looks similar to the sample DCA Application Deactivation.

   Expand the option **Status & Manage** and click **Server** to restart the DSR MP.
5. Log in to the active NOAM VIP and SOAM VIP GUIs.
6. In the NOAM VIP and SOAM VIP GUIs, verify the DCA Application folder and sub-menus.

   On NOAM VIP GUI, expand **Diameter** and click **DCA Framework**, and verify the DCA Application folder no longer exists.

   On SOAM VIP GUI, expand **Diameter** and click **DCA Framework**, and verify the DCA Application folder no longer exists.

7. Close SSH connection to active NOAM VIP GUIs. Log out of the active NOAM VIP GUI, log in to the shell, and close the SSH connections by executing the following command:

   ```
   # exit
   ```

   Close the SSH connection.

   If this procedure fails, contact My Oracle Support (MOS) for assistance.

16.2 DCA Framework Deactivation

All DCA applications must be deactivated before executing the following procedure.

1. Log out of any active NOAM VIP GUI sessions.
2. Establish a secure shell session on the active NOAM VIP GUI by using the XMI VIP address. Log in as `admusr`. Use your SSH client to connect to the server (for example 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>
   ```

3. Change to the DCA activation directory, execute the following command:

   ```
   # cd /usr/TKLC/dsr/prod/maint/loaders/
   ```

4. Execute the DCA activation script. Run the DCA activation script by executing the following command:

   ```
   # ./featureActivateDeactivate
   ```

   Choose **Activate** and **DCA Application** options.

   > **Note**
   >
   > For Tier 3 SOAM, this feature can be deactivated on all SOAMs or a specific SOAM VIP GUI.

   Verify the screen looks similar to the sample DCA Framework Deactivation.
5. Log in to the active NOAM VIP and SOAM VIP GUIs.
6. Verify if the DCA Framework folder no longer exists under the **Diameter** menu.
7. Close SSH connection to active NOAM VIP GUIs. Log out of the active NOAM VIP GUI log in shell and close the SSH connections by executing the following command:

   ```
   # exit
   ```

   Close the SSH connection.

   If this procedure fails, contact My Oracle Support (MOS) for assistance.

17
Post-Deactivation Procedures

To complete a deactivation, complete the Post-Deactivation procedure described below.

17.1 Perform Health Check Post-Feature Deactivation

This procedure performs a health check to determine the health and status of the DSR network and servers.

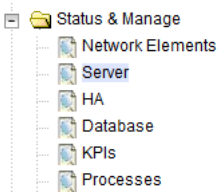
Log in to the NOAM VIP GUI and establish a GUI session on the NOAM server by using the VIP address of the NOAM server.

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

Figure 17-1 Oracle System Log in

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

Figure 17-2 Status and Manage



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

Figure 17-3 Alarms

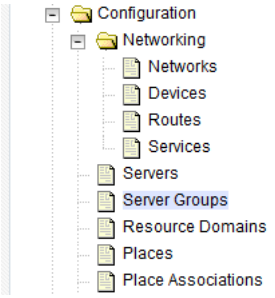
Appl State	Alm	DB	Reporting Status	Proc
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm
Enabled	Norm	Norm	Norm	Norm

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

If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed with the feature activation. If there are Major or Critical alarms present, these alarms should be analyzed before proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms.

5. In the NOAM VIP GUI, verify the server configuration. Expand the option **Configuration** and click **Server Groups**.

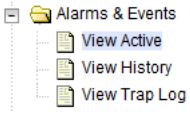
Figure 17-4 Server Groups



Verify the configuration data is correct for your network.

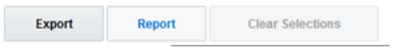
6. In the NOAM VIP GUI, log the current alarms. Expand the **Alarms & Events** option and click **View Active**

Figure 17-5 View Active Alarms



7. Click **Report**

Figure 17-6 Report



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

Figure 17-7 Save or Print

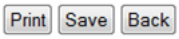
9. In the NOAM VIP GUI, log the alarm history. Expand **Alarms & Events** option and click **View History**.

10. Click **Report**.

Figure 17-8 Report

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

Figure 17-9 Save or Print



If this procedure fails, contact My Oracle Support (MOS) for assistance.

A
DCA Framework Activation

Below is a sample of the DCA Framework Activation procedure.

```
[admusr@HPC07-NO1 loaders]$ ./featureActivateDeactivateTue
 Feb  2 17:47:18 EST 2016::Starting featureActivateDeactivate main...
Start the Automation script , To run the Feature Activation/DeActivation on
Active NO.
You want to Activate or Deactivate the Feature :
1.Activate
2.Deactivate
Enter your choice : 1
List of Feature you can Activate :
1.RBAR
2.FABR
3.Mediation
4.LoadGen
5.GLA
6.MAP Interworking
7.DTLS
8.Dca Framework
9.Dca Application
Enter the choice : 8
Run script to Activate DcaFramework Feature
====================================S-T-A-R-
T==================================
Execution of Activation/Deactivation Process Starts
================================================================================
==
Starting Activation/Deactivation process....
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.DcaFrameworkActivateAsourced script on HPC07-NO1
================================================================================
==
Current server is HA ACTIVE
================================================================================
==
Add Dca Framework KPI group
================================================================================
==
KPI_Group=Dca Framework
Visibility=VIS_ALL
================================================================================
==
Add Dca Framework Measurement groups
================================================================================
==
Meas_Group=Dca Framework Performance
Visibility=VIS_ALL
================================================================================
```

```
==
Add Dca Framework GUI Configuration Permissions.
================================================================================
==
Set Dca Framework Entry in the DcaFrmEngOption table
================================================================================
==
  === changed 1 records ===
================================================================================
==
There is no Standby NOAMP server configured in the Topology
================================================================================
==
The Active SO server configured in the Topology are
================================================================================
==
1. HPC07-SO1
2. ALL SOs
Enter your choice on which SO you want to Activate or Deactivate the
Feature :2
Activate/Deactivate DcaFramework on all SOs configured in the Topology
================================================================================
==
This is a 3 Tier Setup , So run the B sourced loaders on SO server : HPC07-SO1
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.DcaFrameworkActivateBsourced script on HPC07-SO1
FIPS integrity verification test failed.
Add Dca Framework GUI Configuration Permissions.
FIPS integrity verification test failed.
================================================================================
==
Executing the Loaders and Clearing Cache on Standby SO servers.
================================================================================
==
There is no Standby/Spare SOAMP server configured in the Topology
================================================================================
==
```

B
DCA Framework Deactivation

Listed below is a sample of the DCA Framework deactivation procedure:

```
[admusr@HPC07-NO1 loaders]$ ./featureActivateDeactivate
Tue Feb  2 17:50:17 EST 2016::Starting featureActivateDeactivate main...
Start the Automation script , To run the Feature Activation/DeActivation on
Active NO.
You want to Activate or Deactivate the Feature :
1.Activate
2.Deactivate
Enter your choice : 2
List of Feature you can DeActivate :
1.RBAR
2.FABR
3.Mediation
4.LoadGen
5.GLA
6.MAP Interworking
7.DTLS
8.Dca Framework
9.Dca Application
Enter your choice : 8
Run script to Deactivate DcaFramework Feature
====================================S-T-A-R-
T=================================
Execution of Activation/Deactivation Process Starts
================================================================================
==
Starting Activation/Deactivation process....
================================================================================
==
The Active SO server configured in the Topology are
================================================================================
==
1. HPC07-SO1
2. ALL SOs
Enter your choice on which SO you want to Activate or Deactivate the
Feature :2
Verifying feature is activated or not on HPC07-SO1
FIPS integrity verification test failed.
============================================
DCAFRAMEWORK is activated on HPC07-SO1
============================================
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/
load.DcaFrameworkDeactivateAsourced script on HPC07-NO1
================================================================================
==
Current server is HA ACTIVE
================================================================================
```

```
==
There are active dca app on this system. exiting
================================================================================
==
There is no Mate NOAMP server configured in the Topology
================================================================================
==
Activate/Deactivate DcaFramework on all SOs configured in the Topology
================================================================================
==
This is a 3 Tier Setup , So run the B sourced loaders on SO server : HPC07-SO1
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/
load.DcaFrameworkDeactivateBsourced script on HPC07-SO1
FIPS integrity verification test failed.
There are active dca app on this system. exiting
FIPS integrity verification test failed.
================================================================================
==
Executing the Loaders and Clearing Cache on Standby SO servers.
================================================================================
==
There is no Standby/Spare SOAMP server configured in the Topology
================================================================================
========
```

C
DCA Application Activation

Listed below is a sample of the DCA application activation procedure.

```
[admusr@Active-NO loaders]$./featureActivateDeactivate
Wed Mar  1 11:34:03 EST 2017::Starting featureActivateDeactivate main...
Start the Automation script , To run the Feature Activation/DeActivation on
Active NO.
You want to Activate or Deactivate the Feature :
1.Activate
2.Deactivate
Enter your choice : 1
List of Feature you can Activate :
1.RBAR
2.FABR
3.Mediation
4.LoadGen
5.GLA
6.MAP Interworking
7.DTLS
8.DCA Framework
9.DCA Application
Enter the choice : 9
========= Start of Log Data in file /var/TKLC/log/DcaActivationTopLevel.log
=========
====================================S-T-A-R-
T===================================
Log file location: /var/TKLC/log/DcaActivationTopLevel.log
Note:-
In case of any failure please execute /usr/TKLC/dsr/prod/maint/loaders/
deactivate/load.DcaDeactivationTopLevel script to revert the changes.
================================================================================
=====
Execution of Activation Process Starts
================================================================================
=====
Dca framework is activated on the setup..Continuing
Following Dca apps are activated on the system:
First DCA App
1. Recover currently activated Dca Applications
2. Activate a Dca Application
Enter your choice : 2
Enter the long name for the Dca application:Second DCA App
Entered dca name Second DCA App consist of valid characters
Entered Name is Second DCA App
next available dal id is 129
Enter the short name for the Dca application:SDA
length of shortName is 3.continuing..
Entered dca name SDA consist of valid characters
Entered Name is SDA
```

```
==========================================
Verify that Dca Application is in the DalId table
==========================================
dalId=129
birthTime=03/01/2017 11:34:21.000
name=Second DCA App
shortName=DCA:SDA
activated=No
================================================================================
=====
Activation of Dca Application Starts.
================================================================================
=====
Execution of Dca Applicaion Activation Script for Second DCA App[SDA] Starts.
================================================================================
=====
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.DcaActivateAscoped
script on Active-NO
========= Start of Log Data in file /var/TKLC/log/DcaActivateAscoped.log
===========
Server Name  : Active-NO
Server Role  : NETWORK_OAMP
Node Id      : Active-NO
HA State     : Active
Cluster Role : Primary
==========================================
Verify that Dca Application is in the DcaDalId table
==========================================
dalId=129
name=Second DCA App
shortName=SDA
==========================================
Add Dca application entry to the DsrApplication table.
==========================================
Verify that Dca Application is in the table
==========================================
id=129
name=DCA_SDA
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
==============================
Add Dca Application KPI group
==============================
Verify that Dca Application is in the KPIVisibility table
```

```
==========================================
KPI_Group=DCA:SDA
Visibility=VIS_ALL
==================================
Add Dca Application Measurement groups
=======================================
Verify that Dca Application is in the MeasVisibility table
==========================================
Meas_Group=DCA:SDA
Visibility=VIS_ALL
==================================
Add Permission Group headers for Dca Application
================================================
Verify that Dca Application is in the app_permission_groups table
==========================================
_appid=129
group_id=3729
group_name=Second DCA App Configuration Permissions
==================================
Add network configuration parameters for Dca
================================================
Verify that Dca Application is in the DcaAppNetworkUserOption table
==========================================
dalId=129
name=diamAnsSub
value=process_answer
==================================
dalId=129
name=diamRecSub
value=process_request
==================================
dalId=129
name=guestReadOnly
value=true
==================================
dalId=129
name=maxSbrQuery
value=5
==================================
dalId=129
name=opCountEnabled
value=true
==================================
dalId=129
name=opCountHandler
value=3000
==================================
dalId=129
name=opCountMain
value=5000
==================================
dalId=129
name=stateTTL
value=120
====================================E-N-
D=====================================
```

```
Execution status of activation script on Active-NO: PASSED
Please check /var/TKLC/log/DcaActivateAscoped.log for more details.
================================================================================
=====
Starting Activation on StandBy NOAMP Server if it exists in the topology.
================================================================================
=====
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.DcaActivateStandByAscoped script on Standby-NO
FIPS integrity verification test failed.
======= Start of Log Data in file /var/TKLC/log/DcaActivateStandbyAscoped.log
=======
Server Name : Standby-NO
Server Role: NETWORK_OAMP
================================================
Verify that Dca Application is in the DcaDalId table
================================================
dalId=129
name=Second DCA App
shortName=SDA
================================================
Add Dca Application to DsrApplication.
================================================
Verify that Dca Application is in the table
================================================
id=129
name=DCA_SDA
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
================================
Add Permission Group headers for Dca Application
================================================
Verify that Dca Application is in the app_permission_groups table
================================================
_appid=129
group_id=3729
group_name=Second DCA App Configuration Permissions
=====================================================END=====================
========
Execution status of activation script on Standby-NO: PASSED
Please check /var/TKLC/log/DcaActivateStandbyAscoped.log.Standby-NO for more
details.
FIPS integrity verification test failed.
```

```
FIPS integrity verification test failed.
Active-NO is Active and Primary NOAMP Server. So, proceeding with next NOAMP
Server.
======= Activation done on all Network OAMP Servers  =======
======= Starting Activation on System OAM servers =======
Active-SO is Active. So, proceeding with Activation.
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.DcaActivateBscoped
script on Active-SO
FIPS integrity verification test failed.
========= Start of Log Data in file /var/TKLC/log/DcaActivateBscoped.log
============
Server Name : Active-SO
Server Role: SYSTEM_OAM
Node Id    : Active-SO
HA State   : Active
============================================
Verify that Dca Application is in the DcaDalId table
============================================
dalId=129
name=Second DCA App
shortName=SDA
================================
Add Dca application to DsrApplication. If already present then skip.
============================================
Verify that Dca application is in the table
============================================
id=129
name=DCA_SDA
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
============================================================
Add Permission Group headers for Dca app on SOAM server
============================================================
Verify that Dca Application is in the app_permission_groups table
================================================
_appid=129
group_id=3729
group_name=Second DCA App Configuration Permissions
================================================
Add system configuration parameters for Dca
================================================
Verify that Dca Application is in the DcaAppSystemUserOption table
================================================
```

```
dalId=129
name=rtErrAction
value=0
================================
dalId=129
name=rtErrCode
value=
================================
dalId=129
name=rtErrString
value=
================================
dalId=129
name=rtErrVendorId
value=
================================
FIPS integrity verification test failed.
FIPS integrity verification test failed.
======= Start of Log Data in file /var/TKLC/log/DcaActivateStandbyBscoped.log
=======
Server Name : Standby-SO
Server Role: SYSTEM_OAM
Node Id    : Standby-SO
================================================
Add Permission Group headers for Dca Application
================================================
Verify that Dca Application is in the app_permission_groups table
============================================
_appid=129
group_id=3729
group_name=Second DCA App Configuration Permissions
=========================================================END=====================
========
Execution status of activation script on Standby-SO: PASSED
Please check /var/TKLC/log/DcaActivateStandbyBscoped.log.Standby-SO for more
details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
================================================END=============================
========
Execution status of activation script on Active-SO: PASSED
Please check /var/TKLC/log/DcaActivateBscoped.log.Active-SO for more details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
================================================================================
=====
  === changed 1 records ===
============================================
Verify that activated field is udpated for Dca Application in the DalId table
============================================
dalId=129
birthTime=03/01/2017 11:34:21.000
name=Second DCA App
shortName=DCA:SDA
activated=Yes
================================================================================
```

```
=====
Execution of Dca Applicaion Activation Script for Second DCA App[SDA]
completes.
================================================================================
=====
Execution of Dca Applicaion Activation Script complete.
=====================================E-N-
D=======================================
```

D
DCA Application Re-activation

Listed below is a sample of the DCA application re-activation procedure.

```
[admusr@Active-NO loaders]$ ./featureActivateDeactivate
Thu Mar  2 05:17:31 EST 2017::Starting featureActivateDeactivate main...
Start the Automation script , To run the Feature Activation/DeActivation on
Active NO.
You want to Activate or Deactivate the Feature :
1.Activate
2.Deactivate
Enter your choice : 1
List of Feature you can Activate :
1.RBAR
2.FABR
3.Mediation
4.LoadGen
5.GLA
6.MAP Interworking
7.DTLS
8.DCA Framework
9.DCA Application
Enter the choice : 9
========= Start of Log Data in file /var/TKLC/log/DcaActivationTopLevel.log
=========
====================================S-T-A-R-
T===================================
Log file location: /var/TKLC/log/DcaActivationTopLevel.log
Note:-
In case of any failure please execute /usr/TKLC/dsr/prod/maint/loaders/
deactivate/load.DcaDeactivationTopLevel script to revert the changes.
================================================================================
=====
Execution of Activation Process Starts
================================================================================
=====
Dca framework is activated on the setup..Continuing
Following Dca apps are activated on the system:
First DCA App
Second DCA App
1. Recover currently activated Dca Applications
2. Activate a Dca Application
Enter your choice : 1
================================================================================
=====
Recovery of all Currently Activated Dca Application Starts.
================================================================================
=====
Execution of Dca Applicaion Activation Script for First DCA App[FDA] Starts.
================================================================================
```

```
=====
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.DcaActivateAscoped
script on Active-NO
========= Start of Log Data in file /var/TKLC/log/DcaActivateAscoped.log
============
Server Name  : Active-NO
Server Role  : NETWORK_OAMP
Node Id      : Active-NO
HA State     : Active
Cluster Role : Primary
=============================================
Verify that Dca Application is in the DcaDalId table
=============================================
dalId=128
name=First DCA App
shortName=FDA
=========================================================
Add Dca application entry to the DsrApplication table.
=========================================================
Verify that Dca Application is in the table
=============================================
id=128
name=DCA_FDA
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
================================
Add Dca Application KPI group
================================
Given Dca Entry with KPI_Group=DCA:FDA already present in KPIVisibility
table. Skipping.
=============================================
Verify that Dca Application is in the KPIVisibility table
=============================================
KPI_Group=DCA:FDA
Visibility=VIS_ALL
=========================================
Add Dca Application Measurement groups
=========================================
Given Dca Entry with Meas_Group=DCA:FDA already present in MeasVisibility
table. Skipping.
=============================================
Verify that Dca Application is in the MeasVisibility table
=============================================
Meas_Group=DCA:FDA
```

```
Visibility=VIS_ALL
================================================
Add Permission Group headers for Dca Application
================================================
Given Dca Entry with _appid=128 already present in app_permission_groups
table. Skipping.
============================================
Verify that Dca Application is in the app_permission_groups table
============================================
_appid=128
group_id=3728
group_name=First DCA App Configuration Permissions
================================================
Add network configuration parameters for Dca
================================================
Given Dca Entry with name=diamRecSub for dalId=128 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=diamAnsSub for dalId=128 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=stateTTL for dalId=128 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=guestReadOnly for dalId=128 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=maxSbrQuery for dalId=128 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=opCountEnabled for dalId=128 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=opCountMain for dalId=128 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=opCountHandler for dalId=128 already present in
DcaAppNetworkUserOption table. Skipping.
============================================
Verify that Dca Application is in the DcaAppNetworkUserOption table
============================================
dalId=128
name=diamAnsSub
value=process_answer
================================
dalId=128
name=diamRecSub
value=process_request
================================
dalId=128
name=guestReadOnly
value=true
================================
dalId=128
name=maxSbrQuery
value=5
================================
dalId=128
name=opCountEnabled
value=true
================================
dalId=128
name=opCountHandler
```

```
value=3000
================================
dalId=128
name=opCountMain
value=5000
================================
dalId=128
name=stateTTL
value=120
====================================E-N-
D=========================================
 Execution status of activation script on Active-NO: PASSED
Please check /var/TKLC/log/DcaActivateAscoped.log for more details.
================================================================================
=====
Starting Activation on StandBy NOAMP Server if it exists in the topology.
================================================================================
=====
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.DcaActivateStandByAscoped script on Standby-NO
FIPS integrity verification test failed.
======= Start of Log Data in file /var/TKLC/log/DcaActivateStandbyAscoped.log
=======
Server Name : Standby-NO
Server Role: NETWORK_OAMP
============================================
Verify that Dca Application is in the DcaDalId table
============================================
dalId=128
name=First DCA App
shortName=FDA
================================================
Add Dca Application to DsrApplication.
================================================
Verify that Dca Application is in the table
============================================
id=128
name=DCA_FDA
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
================================================
Add Permission Group headers for Dca Application
================================================
```

```
Given Dca Entry with _appid=128 already present in app_permission_groups
table. Skipping.
==========================================
Verify that Dca Application is in the app_permission_groups table
==========================================
_appid=128
group_id=3728
group_name=First DCA App Configuration Permissions
==========================================================END=====================
========
Execution status of activation script on Standby-NO: PASSED
Please check /var/TKLC/log/DcaActivateStandbyAscoped.log.Standby-NO for more
details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
Active-NO is Active and Primary NOAMP Server. So, proceeding with next NOAMP
Server.
======= Activation done on all Network OAMP Servers  =======
======= Starting Activation on System OAM servers =======
Active-SO is Active. So, proceeding with Activation.
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.DcaActivateBscoped
script on Active-SO
FIPS integrity verification test failed.
======== Start of Log Data in file /var/TKLC/log/DcaActivateBscoped.log
============
Server Name : Active-SO
Server Role: SYSTEM_OAM
Node Id    : Active-SO
HA State   : Active
Given Dca application is already in DcaDalId table. Skipping.
==========================================================================
Add Dca application to DsrApplication. If already present then skip.
==========================================================================
Given Dca Entry with name=DCA_FDA already present in DsrApplication table.
Skipping.
==========================================
Verify that Dca application is in the table
==========================================
id=128
name=DCA_FDA
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
==========================================================
```

```
Add Permission Group headers for Dca app on SOAM server
=======================================================
Given Dca Entry with _appid=128 already present in app_permission_groups
table. Skipping.
===============================================
Verify that Dca Application is in the app_permission_groups table
===============================================
_appid=128
group_id=3728
group_name=First DCA App Configuration Permissions
=================================================
Add system configuration parameters for Dca
=================================================
Given Dca Entry with name=rtErrAction for dalId=128 already present in
DcaAppSystemUserOption table. Skipping.
Given Dca Entry with name=rtErrCode for dalId=128 already present in
DcaAppSystemUserOption table. Skipping.
Given Dca Entry with name=rtErrString for dalId=128 already present in
DcaAppSystemUserOption table. Skipping.
Given Dca Entry with name=rtErrVendorId for dalId=128 already present in
DcaAppSystemUserOption table. Skipping.
===============================================
Verify that Dca Application is in the DcaAppSystemUserOption table
===============================================
dalId=128
name=rtErrAction
value=0
================================
dalId=128
name=rtErrCode
value=
================================
dalId=128
name=rtErrString
value=
================================
dalId=128
name=rtErrVendorId
value=
================================
FIPS integrity verification test failed.
FIPS integrity verification test failed.
======= Start of Log Data in file /var/TKLC/log/DcaActivateStandbyBscoped.log
=======
Server Name : Standby-SO
Server Role: SYSTEM_OAM
Node Id    : Standby-SO
=================================================
Add Permission Group headers for Dca Application
=================================================
Given Dca Entry with _appid=128 already present in app_permission_groups
table. Skipping.
===============================================
Verify that Dca Application is in the app_permission_groups table
===============================================
_appid=128
```

```
group_id=3728
group_name=First DCA App Configuration Permissions
=====================================================END=====================
========
Execution status of activation script on Standby-SO: PASSED
Please check /var/TKLC/log/DcaActivateStandbyBscoped.log.Standby-SO for more
details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
================================================END==========================
========
Execution status of activation script on Active-SO: PASSED
Please check /var/TKLC/log/DcaActivateBscoped.log.Active-SO for more details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
================================================================================
=====
  === changed 1 records ===
Verify that activated field is udpated for Dca Application in the DalId table
============================================
dalId=128
birthTime=03/02/2017 02:30:27.000
name=First DCA App
shortName=DCA:FDA
activated=Yes
================================================================================
=====
Execution of Dca Applicaion Activation Script for First DCA App[FDA]
completes.
================================================================================
=====
Execution of Dca Applicaion Activation Script for Second DCA App[SDA] Starts.
================================================================================
=====
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.DcaActivateAscoped
script on Active-NO
========= Start of Log Data in file /var/TKLC/log/DcaActivateAscoped.log
============
Server Name  : Active-NO
Server Role  : NETWORK_OAMP
Node Id      : Active-NO
HA State     : Active
Cluster Role : Primary
============================================
Verify that Dca Application is in the DcaDalId table
============================================
dalId=129
name=Second DCA App
shortName=SDA
=========================================================
Add Dca application entry to the DsrApplication table.
=========================================================
Verify that Dca Application is in the table
============================================
id=129
name=DCA_SDA
```

```
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
================================
Add Dca Application KPI group
================================
Given Dca Entry with KPI_Group=DCA:SDA already present in KPIVisibility
table. Skipping.
============================================
Verify that Dca Application is in the KPIVisibility table
============================================
KPI_Group=DCA:SDA
Visibility=VIS_ALL
========================================
Add Dca Application Measurement groups
========================================
Given Dca Entry with Meas_Group=DCA:SDA already present in MeasVisibility
table. Skipping.
============================================
Verify that Dca Application is in the MeasVisibility table
============================================
Meas_Group=DCA:SDA
Visibility=VIS_ALL
================================================
Add Permission Group headers for Dca Application
================================================
Given Dca Entry with _appid=129 already present in app_permission_groups
table. Skipping.
============================================
Verify that Dca Application is in the app_permission_groups table
============================================
_appid=129
group_id=3729
group_name=Second DCA App Configuration Permissions
================================================
Add network configuration parameters for Dca
================================================
Given Dca Entry with name=diamRecSub for dalId=129 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=diamAnsSub for dalId=129 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=stateTTL for dalId=129 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=guestReadOnly for dalId=129 already present in
DcaAppNetworkUserOption table. Skipping.
```

```
Given Dca Entry with name=maxSbrQuery for dalId=129 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=opCountEnabled for dalId=129 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=opCountMain for dalId=129 already present in
DcaAppNetworkUserOption table. Skipping.
Given Dca Entry with name=opCountHandler for dalId=129 already present in
DcaAppNetworkUserOption table. Skipping.
==============================================
Verify that Dca Application is in the DcaAppNetworkUserOption table
==============================================
dalId=129
name=diamAnsSub
value=process_answer
==================================
dalId=129
name=diamRecSub
value=process_request
==================================
dalId=129
name=guestReadOnly
value=true
==================================
dalId=129
name=maxSbrQuery
value=5
==================================
dalId=129
name=opCountEnabled
value=true
==================================
dalId=129
name=opCountHandler
value=3000
==================================
dalId=129
name=opCountMain
value=5000
==================================
dalId=129
name=stateTTL
value=120
====================================E-N-
D=====================================
Execution status of activation script on Active-NO: PASSED
Please check /var/TKLC/log/DcaActivateAscoped.log for more details.
================================================================================
=====
Starting Activation on StandBy NOAMP Server if it exists in the topology.
================================================================================
=====
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.DcaActivateStandByAscoped script on Standby-NO
FIPS integrity verification test failed.
======= Start of Log Data in file /var/TKLC/log/DcaActivateStandbyAscoped.log
```

```
=======
Server Name : Standby-NO
Server Role: NETWORK_OAMP
=============================================
Verify that Dca Application is in the DcaDalId table
=============================================
dalId=129
name=Second DCA App
shortName=SDA
=============================================
Add Dca Application to DsrApplication.
=============================================
Verify that Dca Application is in the table
=============================================
id=129
name=DCA_SDA
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
=============================================
Add Permission Group headers for Dca Application
=============================================
Given Dca Entry with _appid=129 already present in app_permission_groups
table. Skipping.
=============================================
Verify that Dca Application is in the app_permission_groups table
=============================================
_appid=129
group_id=3729
group_name=Second DCA App Configuration Permissions
=====================================================END=====================
========
Execution status of activation script on Standby-NO: PASSED
Please check /var/TKLC/log/DcaActivateStandbyAscoped.log.Standby-NO for more
details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
Active-NO is Active and Primary NOAMP Server. So, proceeding with next NOAMP
Server.
======= Activation done on all Network OAMP Servers  =======
======= Starting Activation on System OAM servers =======
Active-SO is Active. So, proceeding with Activation.
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.DcaActivateBscoped
script on Active-SO
```

```
FIPS integrity verification test failed.
========= Start of Log Data in file /var/TKLC/log/DcaActivateBscoped.log
============
Server Name : Active-SO
Server Role: SYSTEM_OAM
Node Id    : Active-SO
HA State   : Active
Given Dca application is already in DcaDalId table. Skipping.
=========================================================================
Add Dca application to DsrApplication. If already present then skip.
=========================================================================
Given Dca Entry with name=DCA_SDA already present in DsrApplication table.
Skipping.
==========================================
Verify that Dca application is in the table
==========================================
id=129
name=DCA_SDA
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Graceful
shutdownTimer=5
resultCode=3002
vendorId=0
errorString=
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=DSR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
==========================================================
Add Permission Group headers for Dca app on SOAM server
==========================================================
Given Dca Entry with _appid=129 already present in app_permission_groups
table. Skipping.
==========================================
Verify that Dca Application is in the app_permission_groups table
==========================================
_appid=129
group_id=3729
group_name=Second DCA App Configuration Permissions
==================================================
Add system configuration parameters for Dca
==================================================
Given Dca Entry with name=rtErrAction for dalId=129 already present in
DcaAppSystemUserOption table. Skipping.
Given Dca Entry with name=rtErrCode for dalId=129 already present in
DcaAppSystemUserOption table. Skipping.
Given Dca Entry with name=rtErrString for dalId=129 already present in
DcaAppSystemUserOption table. Skipping.
Given Dca Entry with name=rtErrVendorId for dalId=129 already present in
DcaAppSystemUserOption table. Skipping.
==========================================
Verify that Dca Application is in the DcaAppSystemUserOption table
```

```
==============================================
dalId=129
name=rtErrAction
value=0
================================
dalId=129
name=rtErrCode
value=
================================
dalId=129
name=rtErrString
value=
================================
dalId=129
name=rtErrVendorId
value=
================================
FIPS integrity verification test failed.
FIPS integrity verification test failed.
======= Start of Log Data in file /var/TKLC/log/DcaActivateStandbyBscoped.log
========
Server Name : Standby-SO
Server Role: SYSTEM_OAM
Node Id    : Standby-SO
================================================
Add Permission Group headers for Dca Application
================================================
Given Dca Entry with _appid=129 already present in app_permission_groups
table. Skipping.
==============================================
Verify that Dca Application is in the app_permission_groups table
==============================================
_appid=129
group_id=3729
group_name=Second DCA App Configuration Permissions
=====================================================END=====================
========
Execution status of activation script on Standby-SO: PASSED
Please check /var/TKLC/log/DcaActivateStandbyBscoped.log.Standby-SO for more
details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
============================================END=============================
========
Execution status of activation script on Active-SO: PASSED
Please check /var/TKLC/log/DcaActivateBscoped.log.Active-SO for more details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
================================================================================
=====
  === changed 1 records ===
==============================================
Verify that activated field is udpated for Dca Application in the DalId table
==============================================
dalId=129
birthTime=03/02/2017 05:15:45.000
```

```
name=Second DCA App
shortName=DCA:SDA
activated=Yes
================================================================================
=====
Execution of Dca Applicaion Activation Script for Second DCA App[SDA]
completes.
================================================================================
=====
Execution of Dca Applicaion Activation Script complete.
=====================================E-N-
D=====================================
```

E
DCA Application Deactivation

Listed below is a sample of the DCA application deactivation procedure:

```
[admusr@HPC07-NO1 loaders]$ pwd
/usr/TKLC/dsr/prod/maint/loaders
[admusr@HPC07-NO1 loaders]$ ./featureActivateDeactivate
Tue Feb  2 17:59:21 EST 2016::Starting featureActivateDeactivate main...
Start the Automation script , To run the Feature Activation/DeActivation on
Active NO.
You want to Activate or Deactivate the Feature :
1.Activate
2.Deactivate
Enter your choice : 2
List of Feature you can DeActivate :
1.RBAR
2.FABR
3.Mediation
4.LoadGen
5.GLA
6.MAP Interworking
7.DTLS
8.Dca Framework
9.Dca Application
Enter your choice : 9
==========================  S-T-A-R-T of log DcaDeactivationTopLevel.log
===========
Log file location: /var/TKLC/log/DcaDeactivationTopLevel.log
================================================================================
==Execution of Deactivation Process Starts
================================================================================
==Following Dca apps are activated on the system
1. FDA
2. sda
Enter the name for the Dca application to be deactivated:sda
The name of application selected to deactivate is: sda
  === changed 1 records ===
=========================================================
DalId Table successfully updated with deactivated status.
=========================================================
HPC07-SO1 is Active. So, proceeding with Deactivation.
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/
load.DcaDeactivateBscoped script on HPC07-SO1
FIPS integrity verification test failed.
========= Start of Log Data in file /var/TKLC/log/DcaDeactivateBscoped.log
==========
Server Name : HPC07-SO1
Server Role: SYSTEM_OAM
Node Id    : HPC07-SO1
```

```
HA State   : Active
=====================================================
Remove the ART rules corresponding to the DCA
=====================================================
No rules configured for the current application.
================================================
Remove Dca from DcaAppSystemUserOption table
================================================
  === deleted 5 records ===
=====================================================
Remove Dca Application from DsrApplicationPerMp table
=====================================================
  === deleted 0 records ===
================================================
Remove Dca Application from DsrApplication table
================================================
  === deleted 1 records ===
=========================================================================
Remove permission group headers for Dca Application on SOAM server
=========================================================================
  === deleted 1 records ===
============================================END============================
==
Execution status of deactivation script on HPC07-SO1: PASSED
Please check /var/TKLC/log/DcaDeactivateBscoped.log.HPC07-SO1 for more
details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
=============================================================================
==
 Starting Deactivation on Standby NOAMP server if present in topology.
=============================================================================
==
HPC07-NO1 is Active NOAMP Server. Proceeding with next NOAMP server in the
list.
=============================================================================
==
 Starting Deactivation on Active NOAMP server.
=============================================================================
==
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/
load.DcaDeactivateAscoped script on HPC07-NO1
======== Start of Log Data in file /var/TKLC/log/DcaDeactivateAscoped.log
===========
Server Name  : HPC07-NO1
Server Role  : NETWORK_OAMP
Node Id      : HPC07-NO1
HA State     : Active
Cluster Role : Primary
==================================
Remove Dca Application KPI groups
==================================
  === deleted 1 records ===
=========================================
Remove Dca Application Measurement groups
=========================================
```

```
  === deleted 1 records ===
=====================================================
Remove permission group headers for Dca Application
=====================================================
  === deleted 1 records ===
=============================================
Remove logical to physical sbr db mapping from
DcaLog2PhySbr and DcaLogicalSbr table
=============================================
Remove Dca from DcaLifecycleNoam table
=============================================
  === deleted 0 records ===
=============================================
Remove Dca from DcaAppNetworkUserOption table
=============================================
  === deleted 3 records ===
=============================================
Remove Dca from DcaTrialMp table
=============================================
  === deleted 0 records ===
=============================================
Remove Dca from DsrApplicationPerMp table
=============================================
  === deleted 0 records ===
=============================================
Remove Dca Application from DsrApplication table
=============================================
  === deleted 1 records ===
  === deleted 1 records ===
  === deleted 1 records ===
=====================================END=====================================
Execution status of deactivation script on HPC07-NO1: PASSED
====================Execution of Dca Application Deactivation Script
complete.
====================================E-N-
D====================================
```

F

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity or traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

G

Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com
2. Click Industries.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link. The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings “Network Session Delivery and Control Infrastructure” or “Platforms.”
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the PDF link, select Save target as (or a similar command based on your browser), and save to a local folder.