

Oracle® Communications

Diameter Signaling Router

DSR 8.3 DCA Feature Activation Guide

Release 8.3

E93230-01

September 2018

ORACLE®

Oracle Communications Diameter Signaling Router DCA Feature Activation Procedure, Release 8.3.

Copyright © 2017, 2018 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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



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

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

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

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

See more information on My Oracle Support (MOS).

Table of Contents

Table of Contents	3
List of Tables	4
List of Figures	4
List of Procedures.....	4
1. Introduction.....	5
1.1 References	5
1.2 Acronyms.....	5
1.3 Terminology.....	6
1.4 General Procedure Step Format	6
2. Feature Activation Overview	7
2.1 Definition of Activation for the DCA Feature	7
2.2 Feature Activation Overview	7
3. Feature Deactivation Overview	10
3.1 Pre-Feature Deactivation Overview	10
3.2 Feature Deactivation Execution Overview	10
3.3 Post-Feature Deactivation Overview.....	11
4. Feature Activation Preparation	12
4.1 System Topology Check	12
4.2 Perform Health Check	14
5. Feature Activation	17
5.1 Pre-Activation Procedure — Perform Health Check	17
5.2 Activation Procedures	21
5.3 Post-Activation Procedures	25
6. Feature Deactivation	28
6.1 Pre-Deactivation Procedures	28
6.2 Deactivation Procedures	30
6.3 Post-Deactivation Procedures	33
Appendix A. DCA Framework Activation.....	36
Appendix B. DCA Framework Deactivation.....	38
Appendix C. DCA Application Activation	40
Appendix D. DCA Application Reactivation	48
Appendix E. DCA Application Deactivation	64
Appendix F. My Oracle Support (MOS)	68
Appendix G. Emergency Response	69
Appendix H. Locate Product Documentation on the Oracle Help Center	70

List of Tables

Table 1. Acronyms	5
Table 2. Terminology	6
Table 3. Behavior of DCA Framework and Application Activation and Deactivation.....	7
Table 4. Pre-Feature Activation Overview	7
Table 5. DCA Framework Activation Execution Overview	8
Table 6. DCA Application Activation Execution Overview	8
Table 7. Post-Feature Activation Overview.....	9
Table 8. Pre-Feature Deactivation Overview	10
Table 9. DCA Application Deactivation Overview	10
Table 10. DCA Framework Deactivation Overview	11
Table 11. Post-Feature Deactivation Overview	11

List of Figures

Figure 1. Example of a Procedure Step.....	6
--	---

List of Procedures

Procedure 1: System Topology Check	12
Procedure 2: Perform Health Check	14
Procedure 3: Perform Health Check (Pre-Feature Activation).....	17
Procedure 4: DCA Framework Activation	21
Procedure 5: DCA Application Activation.....	22
Procedure 6: DCA Application Reactivation	23
Procedure 7: Perform Health Check (Post-Feature Activation)	25
Procedure 8: Perform Health Check (Pre-Feature Deactivation)	28
Procedure 9: DCA Application Deactivation	30
Procedure 10: DCA Framework Deactivation	31
Procedure 11: Perform Health Check (Post-Feature Deactivation).....	33

1. Introduction

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

This document also provides a procedure to deactivate DCA framework and applications after it has been activated. Refer to Section 6 for a discussion of deactivation.

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.

1.1 References

- [1] DSR 8.3 Software Installation and Configuration Procedure 1/2
- [2] DSR 8.3 C-Class Software Installation and Configuration Procedure 2/2
- [3] DSR 8.3 Software Upgrade Guide

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

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

Acronym	Definition
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface

1.3 Terminology

Table 2. Terminology

Term	Definition
NOAM	Network Operations and Maintenance
SOAM	System Operations and Maintenance

1.4 General Procedure Step Format

Figure 1 illustrates the general format of procedure steps as they appear in this document. Where it is necessary to explicitly identify the server on which a particular step is to be taken, the server name is given in the title box for the step (e.g., **ServerX** in Figure 1).

Each step has a checkbox for every command within the step that the technician should check to keep track of the progress of the procedure.

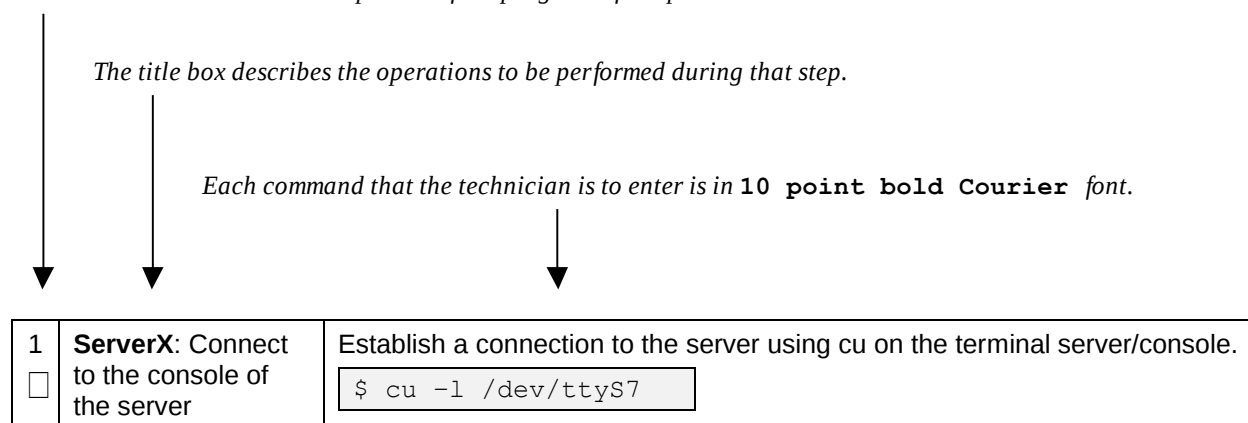


Figure 1. Example of a Procedure Step

2. Feature Activation Overview

This section lists the required materials and information needed to execute the feature activation. In addition, Table 4 through Table 11 provide estimates of the time required to execute the procedure. These tables can be used to estimate the total time necessary to complete the feature activation. The timing values shown are estimates only – use these tables to plan the timing of the activation, **not** to execute the procedure. The detailed procedure steps to be executed begin in Section 4.

2.1 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 software required to run DCA is available by default as part of a DSR installation or upgrade. 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. Behavior of DCA Framework and Application Activation and Deactivation

SL No	DCA	Behavior
1	DCA Framework Activation	Section 5.2.1
2	DCA Application Activation	Section 5.2.2
3	DCA Application Deactivation	Section 6.2.1
4	DCA Framework Deactivation	Section 6.2.2

2.2 Feature Activation Overview

2.2.1 Pre-Feature Activation Overview

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

Table 4. Pre-Feature Activation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation
	This Step	Cum.	
System Topology Check (Procedure 1)	0:10-0:30	0:20-1:00	- Verify network element configuration data - Verify system group configuration data
Perform Health Check (Procedure 2)	0:01-0:05	0:21-1:05	- Verify DSR release - Verify server status - Log all current alarms

2.2.2 Feature Activation Execution Overview

The procedures shown in the following table are executed inside a single maintenance window. 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. DCA Framework Activation Execution Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution	Impact
	This Step	Cum.		
Perform Health Check (Procedure 3)	0:01-0:05	0:01-0:05	- Verify DSR release - Verify proper DCA state - Verify server status - Log all current alarms	None
DCA Framework Activation (Procedure 4)	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 NOAMs	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 6. DCA Application Activation Execution Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution	Impact
	This Step	Cum.		
DCA Application Activation (Procedure 5)	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

2.2.3 Post-Feature Activation Overview

The procedures shown 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 7. Post-Feature Activation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution	Impact
	This Step	Cum.		
Perform Health Check (Procedure 7)	0:01-0:05	0:01-0:05	• Verify Server status • Log all current alarms	DCA has been activated on DSR

3. Feature Deactivation Overview

3.1 Pre-Feature Deactivation Overview

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

Table 8. Pre-Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution	Impact
	This Step	Cum.		
Perform Health Check (Procedure 8)	0:01- 0:05	0:01-0:05	• Verify DSR release • Verify proper DCA state • Verify server status • Log current alarms	None

3.2 Feature Deactivation Execution Overview

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

Table 9. DCA Application Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution	Impact
	This Step	Cum.		
Deactivation Setup	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
Deactivation (Procedure 9)	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 10. DCA Framework Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution	Impact
	This Step	Cum.		
Deactivation Setup	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
Deactivation (Procedure 10)	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 NOAM	DCA framework is deactivated on DSR

3.3 Post-Feature Deactivation Overview

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

Table 11. Post-Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution
	This Step	Cum.	
Perform Health Check (Procedure 11)	0:01-0:05	0:01-0:05	• Verify server status. • Log all current alarms.

4. 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.

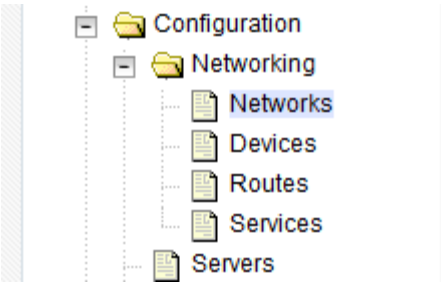
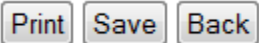
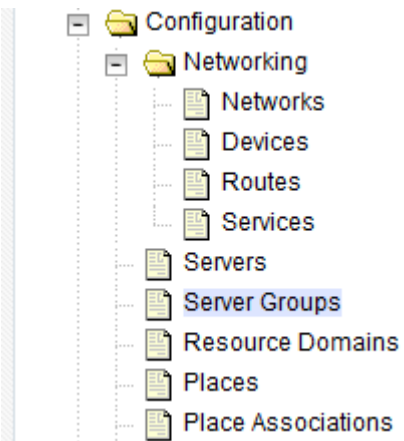
This section provides detailed procedures to prepare a system for DCA feature activation. These procedures are executed outside a maintenance window.

4.1 System Topology Check

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

Procedure 1: System Topology Check

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

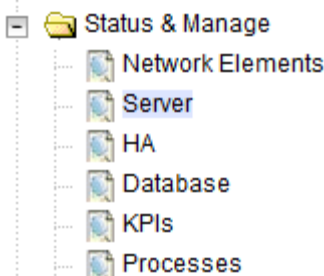
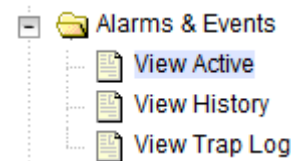
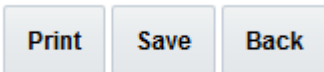
STEP #	Procedure	Description
2. ☐	NOAM VIP GUI: Verify network configuration data	Navigate to Configuration -> Networking -> Networks.  Click Report.  Verify the configuration data is correct for your network. Save or Print this report to keep copies for future reference. 
3. ☐	NOAM VIP GUI: Verify server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

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

Procedure 2: Perform Health Check

STEP #	Procedure	Description
This procedure provides steps to perform needed health checks. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: http://<Primary_NOAM_VIP_IP_Address> Login as the guiadmin user: 
2. ☐	NOAM VIP GUI: Verify DSR release	Navigate to Administration -> Software Versions to verify the Eagle XG DSR RPM version shows version 8.0.0 or greater.

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

STEP #	Procedure	Description
5. ☐	NOAM VIP GUI: Log alarm history	Navigate to Alarms & Events -> View History. Click Report. Export Report Clear Selections Save or Print this report to keep copies for future reference. Print Save Back

5. Feature Activation

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

***** WARNING *****

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

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

Read the following notes on feature activation procedures:

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

5.1 Pre-Activation Procedure — Perform Health Check

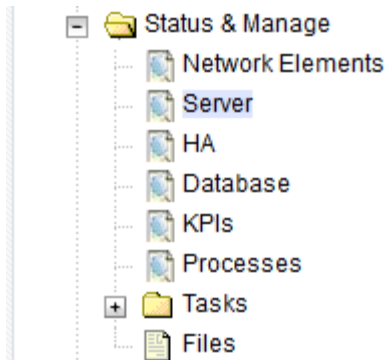
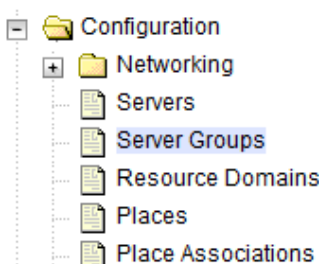
This procedure is used to determine the health and status of the network and servers. This must be executed at the start of every maintenance window.

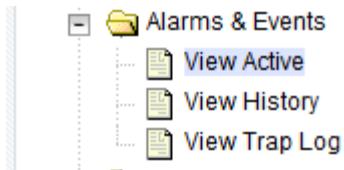
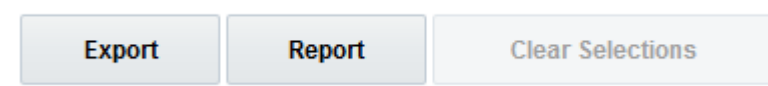
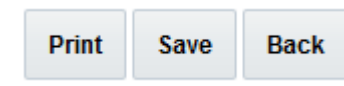
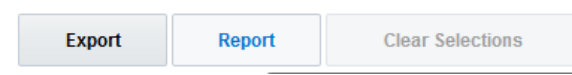
Note: The Health Check procedure below is the same as the Health Check procedure described in Section 4.2 when preparing for feature activation, but it is repeated here to emphasize that it is being re-executed if Section 4.2 was performed outside the maintenance window.

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

STEP #	Procedure	Description
		This procedure performs needed health checks.
		Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.
		If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Description
1. ☐	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: http://<Primary_NOAM_VIP_IP_Address> Login as the guiadmin user:  Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
2. ☐	NOAM (2-Tiered) VIP GUI: Verify DCA Framework folder is not present	Under Main Menu -> Diameter , verify the DCA Framework folder is NOT present.
3. ☐	SOAM (3-Tiered) VIP GUI: Verify DCA Framework folder is not present	Under Main Menu -> Diameter , verify the DCA Framework folder is NOT present.

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

STEP #	Procedure	Description																																				
6. ☐	NOAM VIP GUI: Log current alarms	Navigate to Alarms & Events -> View Active.  Click Report.  Save or Print this report to keep copies for future reference. 																																				
7. ☐	NOAM VIP GUI: Log alarm history	Navigate to Alarms & Events -> View History. Click Report.  Save or Print this report to keep copies for future reference. 																																				
8. ☐	NOAM VIP GUI: Check the Upgrade Acceptance status on all servers	Navigate to Administration -> Software Management -> Upgrade. Verify the Upgrade State column does not show ACCEPT or REJECT. Note: Upgrade must be accepted on all servers before activating DCA. DSR_DR_NO_SG DSR_NO_SG DSR_SO_SG <table><tr><th>Hostname</th><th>Upgrade State</th><th>OAM HA Role</th><th>Server Role</th><th>Function</th><th>Application Version</th></tr><tr><th></th><th>Server Status</th><th>Appl HA Role</th><th>Network Element</th><th></th><th>Upgrade ISO</th></tr><tr><td>DSR-NO2</td><td>Ready</td><td>Standby</td><td>Network OAM&P</td><td>OAM&P</td><td>8.0.0.0-80.18.1</td></tr><tr><td></td><td>Norm</td><td>N/A</td><td>NO_SetupA</td><td></td><td></td></tr><tr><td>DSR-NO-1</td><td>Ready</td><td>Active</td><td>Network OAM&P</td><td>OAM&P</td><td>8.0.0.0-80.18.1</td></tr><tr><td></td><td>Norm</td><td>N/A</td><td>NO_SetupA</td><td></td><td></td></tr></table> Upgrade State should be Ready. If the Upgrade State is ACCEPT OR REJECT, follow [2] DSR 8.3 C-Class Software Installation and Configuration Procedure 2/2 or [3] DSR 8.3 Software Upgrade Guide (whichever applies) to accept the upgrade on all servers before activating DCA.	Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version		Server Status	Appl HA Role	Network Element		Upgrade ISO	DSR-NO2	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0-80.18.1		Norm	N/A	NO_SetupA			DSR-NO-1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0-80.18.1		Norm	N/A	NO_SetupA		
Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version																																	
	Server Status	Appl HA Role	Network Element		Upgrade ISO																																	
DSR-NO2	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0-80.18.1																																	
	Norm	N/A	NO_SetupA																																			
DSR-NO-1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0-80.18.1																																	
	Norm	N/A	NO_SetupA																																			

5.2 Activation Procedures

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

5.2.1 DCA Framework Activation

Procedure 4: DCA Framework Activation

STEP #	Procedure	Description
This procedure verifies that the feature activation steps have been completed. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Logout	Log out of any active NOAM GUI sessions.
2. ☐	Establish a secure shell session on the active NOAM	Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as the admusr. Use your SSH client to connect to the server (ex. Putty). Note: You must consult your own software client's documentation to learn how to launch a connection. For example: <pre># ssh <active NO XMI VIP Address></pre>
3. ☐	DCA Activation: Change directory	Change to the following directory: <pre>\$ cd /usr/TKLC/dsr/prod/maint/loaders/activate</pre>
4. ☐	DCA Activation: Execute the DCA activation script	Run the DCA activation script by executing the following command: <pre># ./featureActivateDeactivate</pre> 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 Appendix A.
5. ☐	NOAM VIP and SOAM VIP GUIs: Login	Log into the active NOAM and SOAM GUIs.

STEP #	Procedure	Description
6. ☐	NOAM VIP and SOAM VIP GUIs: Verify the DCA Framework folder and Configuration sub-menu	On NOAM, verify the DCA Framework folder displays under the DSR Main Menu with Configuration as a sub-menu. On SOAM, verify the DCA Framework folder displays under the DSR Main Menu with Configuration as a sub-menu.
7. ☐	Close SSH connection to active NOAMS	Log out of the active NOAM login shell and close the SSH connections by executing the following command: <pre># exit</pre> Close the SSH connection

5.2.2 DCA Application Activation

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

Procedure 5: DCA Application Activation

STEP #	Procedure	Description
This procedure verifies that the global admin has been enabled.. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Logout	Log out of any active NOAM GUI sessions.
2. ☐	Establish a secure shell session on the active NOAM	Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as the admusr. Use your SSH client to connect to the server (ex. Putty). Note: You must consult your own software client's documentation to learn how to launch a connection. For example: <pre># ssh <active NO XMI VIP Address></pre>
3. ☐	Change to the DCA activation directory	<pre># cd /usr/TKLC/dsr/prod/maint/loaders/</pre>

STEP #	Procedure	Description
4. ☐	Execute the DCA activation script	Execute the feature activation script: <pre># ./featureActivateDeactivate</pre> Choose Activate and DCA Application. 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 Appendix C. Navigate to Status & Manage -> Server to restart the DSR MP.
5. ☐	NOAM VIP and SOAM VIP GUIs: Login	Log into the active NOAM and SOAM GUIs.
6. ☐	NOAM VIP and SOAM VIP GUIs: Verify the DCA Application folder and sub-menus	On NOAM, 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, 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 NOAMs	Log out of the active NOAM login shell and close the SSH connections by executing the following command: <pre># exit</pre> Close the SSH connection

5.2.3 DCA Application Reactivation

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

Procedure 6: DCA Application Reactivation

STEP#	Procedure	Description
		This procedure verifies that the global admin has been enabled.. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

STEP#	Procedure	Description
1. ☐	NOAM VIP GUI: Logout	Log out of any active NOAM GUI sessions.
2. ☐	Establish a secure shell session on the active NOAM	Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as the admusr. Use your SSH client to connect to the server (ex. Putty). Note: You must consult your own software client's documentation to learn how to launch a connection. For example: <pre># ssh <active NO XMI VIP Address></pre>
3. ☐	Change to the DCA activation directory	<pre># cd /usr/TKLC/dsr/prod/maint/loaders/</pre>
4. ☐	Execute the DCA activation script	Execute the feature activation script: <pre># ./featureActivateDeactivate</pre> Choose Activate and DCA Application. 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 Appendix C. Navigate to Status & Manage -> Server to restart the DSR MP.
5. ☐	NOAM VIP and SOAM VIP GUIs: Login	Log into the active NOAM and SOAM GUIs.
6. ☐	NOAM VIP and SOAM VIP GUIs: Verify the DCA Application folder and sub-menus	On NOAM, 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, 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 NOAMs	Log out of the active NOAM login shell and close the SSH connections by executing the following command: <pre># exit</pre> Close the SSH connection

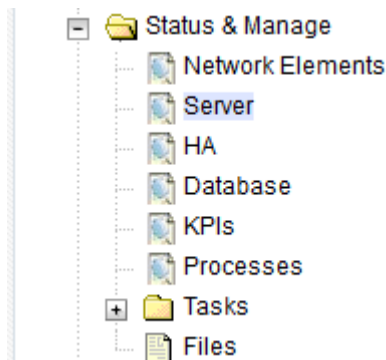
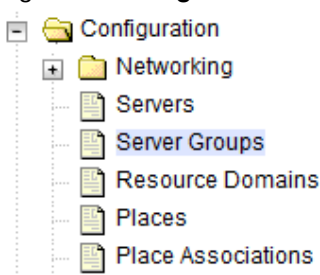
5.3 Post-Activation Procedures

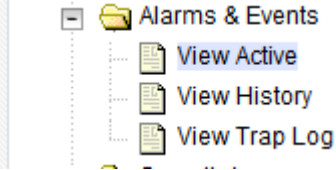
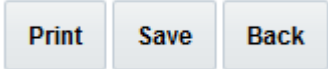
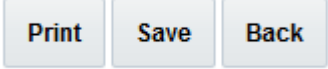
5.3.1 Perform Health Check

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

Procedure 7: Perform Health Check (Post-Feature Activation)

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

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

STEP#	Procedure	Description
4. ☐	NOAM VIP GUI: Log current alarms	Navigate to Alarms & Events -> View Active.  Click Report.  Save or Print this report to keep copies for future reference. 
5. ☐	NOAM VIP GUI: Log alarm history	Navigate to Alarms & Events -> View History. Click Report.  Save or Print this report to keep copies for future reference. 

6. Feature Deactivation

6.1 Pre-Deactivation Procedures

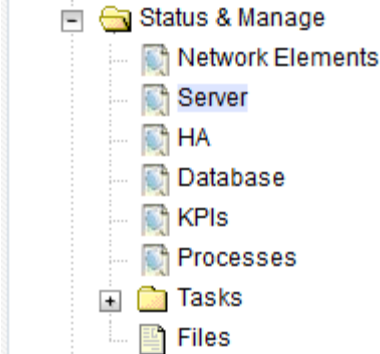
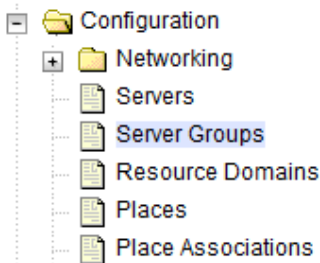
Before beginning the feature deactivation, complete the Pre-Deactivation procedure below.

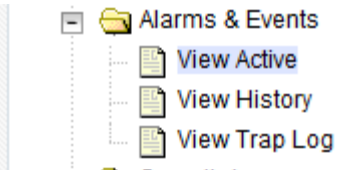
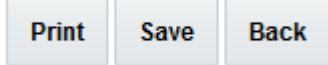
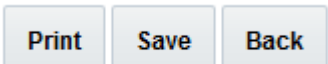
6.1.1 Perform Health Check

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

Procedure 8: Perform Health Check (Pre-Feature Deactivation)

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

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

STEP#	Procedure	Description
4. ☐	NOAM VIP GUI: Log current alarms	Navigate to Alarms & Events -> View Active.  Click Report.  Save or Print this report to keep copies for future reference. 
5. ☐	NOAM VIP GUI: Log alarm history	Navigate to Alarms & Events -> View History. Click Report.  Save or Print this report to keep copies for future reference. 

6.2 Deactivation Procedures

6.2.1 DCA Application Deactivation

Procedure 9: DCA Application Deactivation

STEP #	Procedure	Decription
This procedure verifies that the feature deactivation steps have been completed . Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Logout	Log out of any active NOAM GUI sessions.
2. ☐	Establish a secure shell session on the active NOAM	Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as the admusr. Use your SSH client to connect to the server (ex. Putty). Note: You must consult your own software client's documentation to learn how to launch a connection. For example: <pre># ssh <active NO XMI VIP Address></pre>

STEP #	Procedure	Description
3. ☐	Change to the DCA activation directory	# cd /usr/TKLC/dsr/prod/maint/loaders/
4. ☐	Execute the DCA activation script	Execute the feature activation script: # ./featureActivateDeactivate Choose Deactivate and DCA Application . When asked, Enter the name for the DCA application to be deactivated . Verify the screen looks similar to Appendix D. Navigate to Status & Manage -> Server to restart the DSR MP.
5. ☐	NOAM VIP and SOAM VIP GUIs: Login	Log into the active NOAM and SOAM GUIs.
6. ☐	NOAM VIP and SOAM VIP GUIs: Verify the DCA Application folder and sub-menus	On NOAM, navigate to Diameter -> DCA Framework and verify the DCA Application folder no longer exists. On SOAM, navigate to Diameter -> DCA Framework and verify the DCA Application folder no longer exists.
7. ☐	Close SSH connection to active NOAMs	Log out of the active NOAM login shell and close the SSH connections by executing the following command: # exit Close the SSH connection

6.2.2 DCA Framework Deactivation

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

Procedure 10: DCA Framework Deactivation

STEP #	Procedure	Description
This procedure verifies that the DCA Framework has been disabled. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	NOAM VIP GUI: Logout	Log out of any active NOAM GUI sessions.
2. ☐	Establish a secure shell session on the active NOAM	Establish a secure shell session on the active NOAM by using the XMI VIP address. Login as the admusr. Use your SSH client to connect to the server (ex. Putty). Note: You must consult your own software client's documentation to learn how to launch a connection. For example: <pre># ssh <active NO XMI VIP Address></pre>

STEP #	Procedure	Description
3. ☐	Change to the DCA activation directory	# cd /usr/TKLC/dsr/prod/maint/loaders/
4. ☐	Execute the DCA activation script	Execute the feature activation script: # ./featureActivateDeactivate Choose Deactivate and DCA Application . Note: For Tier 3 SOAM, this feature can be deactivated on all SOAMs or a specific SOAM. Verify the screen looks similar to Appendix E.
5. ☐	Log into Active NOAM and SOAM GUI	Log into the Active NOAM and SOAM GUI.
6. ☐	Verify the DCA Framework folder	Verify the DCA Framework folder no longer exists under the Diameter menu.
7. ☐	Close SSH connection to active NOAMS	Log out of the active NOAM login shell and close the SSH connections by executing the following command: # exit Close the SSH connection

6.3 Post-Deactivation Procedures

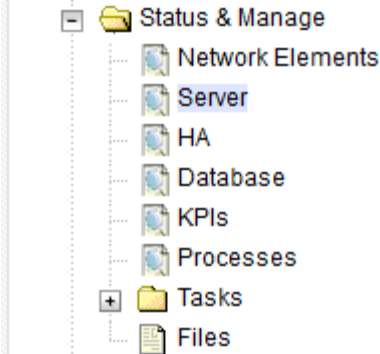
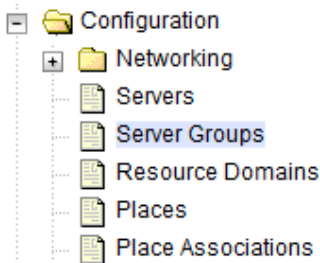
To complete a deactivation, complete the Post-Deactivation procedure below.

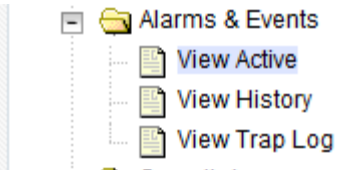
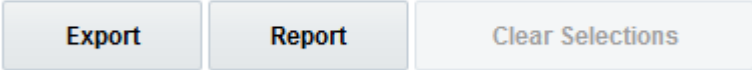
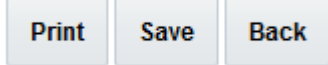
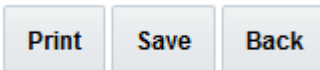
6.3.1 Perform Health Check

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

Procedure 11: Perform Health Check (Post-Feature Deactivation)

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

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

STEP #	Procedure	Description
4. ☐	NOAM VIP GUI: Log current alarms	Navigate to Alarms & Events -> View Active.  Click Report.  Save or Print this report to keep copies for future reference. 
5. ☐	NOAM VIP GUI: Log alarm history	Navigate to Alarms & Events -> View History. Click Report.  Save or Print this report to keep copies for future reference. 

Appendix A. DCA Framework Activation

```
[admusr@HPC07-N01 loaders]$ ./featureActivateDeactivate
Tue 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-N01
=====
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-S01
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-S01
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/load.DcaFrameworkActivateB sourced
script on HPC07-S01
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
=====

```

Appendix B. DCA Framework Deactivation

```
[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-S01
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-S01
FIPS integrity verification test failed.
=====
DCAFRAMEWORK is activated on HPC07-S01
=====
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-S01
Executing
/usr/TKLC/dsr/prod/maint/loaders/deactivate/load.DcaFrameworkDeactivateB sourced script
on HPC07-S01
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
=====
```

Appendix C. DCA Application Activation

```
[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.DcaActivateAsscoped script on
Active-NO
===== Start of Log Data in file /var/TKLC/log/DcaActivateAsscoped.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 updated 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=====

```

Appendix D. DCA Application Reactivation

```
[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.DcaActivateAsScoped script on
Active-NO
===== Start of Log Data in file /var/TKLC/log/DcaActivateAsScoped.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/DcaActivateStandbyAsScoped.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 updated 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/DcaActivateStandbyAsScoped.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 updated 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 Application Activation Script for Second DCA App[SDA] completes.
=====
Execution of Dca Application Activation Script complete.
=====E-N-D=====

```

Appendix E. DCA Application Deactivation

```
[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-S01 is Active. So, proceeding with Deactivation.
FIPS integrity verification test failed.
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/load.DcaDeactivateBscoped script
on HPC07-S01
FIPS integrity verification test failed.
```

```

===== Start of Log Data in file /var/TKLC/log/DcaDeactivateBscoped.log =====
Server Name : HPC07-S01
Server Role: SYSTEM_OAM
Node Id      : HPC07-S01
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-S01: PASSED
Please check /var/TKLC/log/DcaDeactivateBscoped.log.HPC07-S01 for more details.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
=====
Starting Deactivation on Standby NOAMP server if present in topology.
=====
HPC07-N01 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.DcaDeactivateAsscoped script
on HPC07-N01
===== Start of Log Data in file /var/TKLC/log/DcaDeactivateAsscoped.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=====
```

Appendix F. My Oracle Support (MOS)

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

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

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

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

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

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

Appendix G. 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/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Appendix H. 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 similar command based on your browser), and save to a local folder.