

Oracle® Communications

Diameter Signaling Router Range-Based Address Resolution Feature Activation Guide



Release 8.6.0.0.0

F56021-01

April 2022

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

ORACLE®

F56021-01

Copyright © 2000, 2022, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

Contents

1	Introduction	
	Purpose and Scope	1-1
	References	1-1
2	Feature Activation Overview	
	Definition of Activation for the RBAR Feature	2-1
	Feature Activation Overview	2-1
	Pre-feature Activation Overview	2-1
	Feature Activation Execution Overview	2-2
	Post-Feature Activation Review	2-3
3	Feature Deactivation Overview	
	Pre-Feature Deactivation Overview	3-1
	Feature Deactivation Execution Overview	3-1
	Post Feature Deactivation Overview	3-3
4	Feature Activation Procedure	
	System Topology Check	4-1
	Perform Health Check	4-3
5	Feature Activation	
	Pre-Activation Procedures	5-1
	Pre-Feature Activation Health Check	5-1
	Activation Procedures	5-6
	RBAR Feature Activation	5-6
	Post-Activation Procedures	5-11
	Post-Feature Activation Health Check	5-11

6 Feature Deactivation

Pre-Deactivation Procedures	6-1
Pre-Feature Deactivation Health Check	6-1
Deactivation Procedures	6-5
RBAR Feature Deactivation	6-5
Post-Deactivation Procedures	6-10
Post-Feature Deactivation Health Check	6-10

7 Engineering Notes

Sample Output of Activation (Active NOAM)	7-1
Sample Output of De-Activation (Active NOAM)	7-5

A Emergency Response

B Locate Product Documentation on the Oracle Help Center Site

My Oracle Support

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

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

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
 - For Technical issues such as creating a new Service Request (SR), select **1**.
 - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

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

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

Acronyms

An alphabetized list of acronyms used in the document:

Table Acronyms

Acronyms	Definition
BNS	Broadband Networking Solutions
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
RBAR	Range-Based Address Resolution
SOAM	System OAM
SSH	Secure Shell
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface

What's New in this Guide

No updates made to this document in this release.

1

Introduction

Purpose and Scope

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

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

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

References

1. Diameter Signaling Range-Based Resolution (RBAR) User's Guide, Latest Revision

2

Feature Activation Overview

This section lists the required materials and information needed to execute the feature activation. In addition, Table 3 through Table 8 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 5.

Definition of Activation for the RBAR Feature

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

All software required to run RBAR is available by default as part of a DSR release 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.

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

After feature activation, all selectable RBAR-related menu items are present on the SOAM GUI, allowing full RBAR configuration and provisioning. Specifically, the top-level RBAR folder is visible on the Main Menu, and a new entry is added to the Diameter -> Maintenance -> Applications table, showing RBAR and its state. After activation, the DA-MP(s) are prepared to act on RBAR configuration and provisioning information entered at and replicated from the NOAM.

WARNING:

Once the RBAR feature is activated, it is not automatically enabled. Activation simply means the mechanism for provisioning RBAR behavior is in place. But the DA-MP(s) accepts and acts on RBAR provisioning information only after RBAR has been enabled (via the Diameter -> Maintenance -> Applications screen). RBAR should not be enabled until after the appropriate provisioning data has been entered. RBAR provisioning is beyond the scope of this document.

Feature Activation Overview

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 2-1 Pre-Feature Activation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Preparation	Impact
	This Step	Cum.		
System Topology Check (Procedure 1)	0:20	0:20	<ul style="list-style-type: none"> Verify Network Element Configuration data. Verify System Group Configuration data. Analyze and plan DA-MP restart sequence. 	None
Perform Health Check (Procedure 2)	0:05	0:25	<ul style="list-style-type: none"> Verify DSR release. Verify server status. Log all current alarms. 	None

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 2-2 Feature Activation Execution Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution	Impact
	This Step	Cum.		
Perform Health Check (Procedure 3)	0:05	0:05	<ul style="list-style-type: none"> Verify DSR release. Verify proper RBAR feature state. Verify server status. Log all current alarms. 	None

Table 2-2 (Cont.) Feature Activation Execution Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Execution	Impact
Feature Activation(Procedure 4)	0:20	0.25	<ul style="list-style-type: none"> • Log out of NOAM or SOAM GUI. • SSH to active NOAM. • Login as admusr. • Change directory to /usr/TKLC/dsr/prod/maint/loaders/. • Execute the feature activation script. • Log into SOAM GUI. • Verify the RBAR Folder. • Restart each active DAMP server • Verify Maintenance screen. • Log into NOAM GUI. • Verify Maintenance screen. • Close SSH connections to NOAM. 	RBAR is activated

Post-Feature Activation Review

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 2-3 Post-Feature Activation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Feature Activation Completion	Impact
	This Step	Cum.		
Perform Health Check (Procedure 5)	0:05	0:05	<ul style="list-style-type: none">• Verify server status.• Log all current alarms.	RBAR has been activated on DSR

3

Feature Deactivation Overview

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 3-1 Pre-Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Deactivation Procedures	Impact
	This Step	Cum.		
Perform Health Check (Procedure 6)	0:05	0:05	<ul style="list-style-type: none">• Verify DSR release.• Verify proper RBAR feature state.• Verify server status.• Log current alarms.	None

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 3-2 Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Deactivation Procedures	Impact
	This Step	Cum.		

Table 3-2 (Cont.) Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Deactivation Procedures	Impact
Deactivation Setup	0:30	0:30	<ul style="list-style-type: none"> • The reason to deactivate has a direct impact on any additional back-out preparation that must be done. Since not all possible reasons can be predicted ahead of time, only estimates are given here. Execution time will vary. 	None
Deactivation (Procedure 7)	0:20	0:50	<ul style="list-style-type: none"> • Log out of active NOAM/ SOAM GUI. • SSH into active NOAM. • Login as admusr • Change directory to /usr/ TKLC/dsr/ prod/maint/ loaders/ • Execute the feature deactivation script. • Log into NOAM or SOAM GUI. • Verify the FABR folder. • Restart each active DA-MP server. • Log into NOAM GUI • Verify Maintenance screen. 	RBAR is deactivated

Post Feature Deactivation Overview

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

Table 3-3 Post-Feature Deactivation Overview

Procedure	Elapsed Time (Hours:Minutes)		Activity Deactivation Procedures	Impact
	This Step	Cum.		
Perform Health Check (Procedure 8)	0:05	0:05	<ul style="list-style-type: none">• Verify server status.• Log all current alarms.	None

4

Feature Activation Procedure

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

System Topology Check

Procedure 1: System Topology Check

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

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

Figure 4-1 Oracle System Login

ORACLE®

Oracle System Login Mon Jul 11 13:59:37 2016 EDT

Log In

Enter your username and password to log in

Username:

Password:

Change password

Welcome to the Oracle System Login.

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

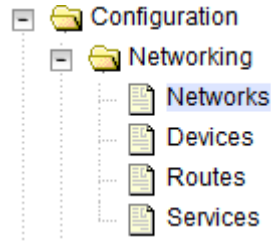
Unauthorized access is prohibited.

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

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

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

Figure 4-2 Navigation to Networks



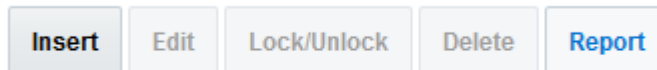
6. Select the site network element tab.

Figure 4-3 Network Element Tag

Network Name	Network Type	Default	Locked
<i>XMI</i>	<i>OAM</i>	<i>Yes</i>	<i>Yes</i>
<i>IMI</i>	<i>OAM</i>	<i>No</i>	<i>Yes</i>
<i>xsi1</i>	<i>Signaling</i>	<i>No</i>	<i>No</i>
<i>xsi2</i>	<i>Signaling</i>	<i>No</i>	<i>No</i>
<i>xsi3</i>	<i>Signaling</i>	<i>No</i>	<i>No</i>

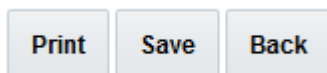
7. Click **Report**

Figure 4-4 Report



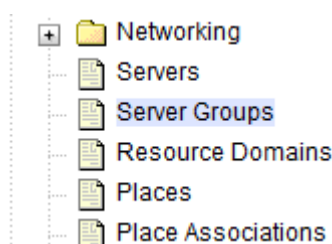
8. Verify if the configuration data is correct for your network. **Save** or **Print** this report to keep copies for future reference.

Figure 4-5 Save or Print



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

Figure 4-6 Server Groups



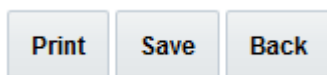
10. Click **Report**.

Figure 4-7 Report



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

Figure 4-8 Save or Print



12. Analyze and plan the DA-MP re-start sequence. Analyze the system topology and plan for any DA-MPs, which will be out-of-service during the feature activation sequence. Analyze system topology gathered in [Step 5](#) and [Step 9](#). Determine exact sequence which DA-MP servers will be restarted (with the expected out-of-service periods).

 **Note:**

It is recommended that no more than 50% of the MPs be restarted at once.

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

Perform Health Check

Procedure 2: Perform Health Check (Feature Activation Preparation)

This procedure is part of feature activation preparation and is used to determine the health and status of the DSR release network and servers. This may be executed multiple times but must also be executed at least once within the time frame of 24-36 hours before the start of the maintenance window in which the feature activation will take place.

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

1. Open the web browser and enter the URL, `http://<Primary_NOAM_VIP_IP_Address>`

2. Log in as the `guiadmin` user.

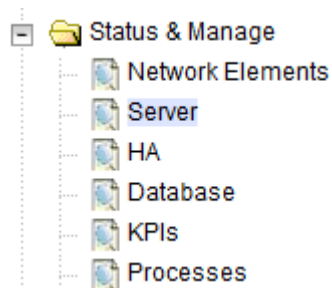
Figure 4-9 Oracle System Login



Verify the server status.

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

Figure 4-10 Server



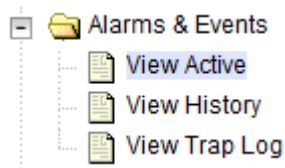
4. Verify if Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).

Figure 4-11 Server Status

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

Do not proceed to feature activation if any of the above states are not `Norm`. If any of these are not `Norm`, corrective action should be taken to restore the `non-Norm` status to `Norm` before proceeding with the feature activation. If the Alarm (Alm) status is not `Norm` but only Minor alarms are present, it is acceptable to proceed with the feature activation. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms. Contact My Oracle Support (MOS) for assistance as necessary.

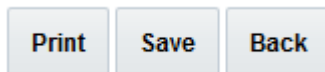
5. Log current alarms, Expand **Alarms & Events** option and click **View Active**.

Figure 4-12 Alarm and Events

6. Click **Report**.

Figure 4-13 Report

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

Figure 4-14 Save

 **Note:**

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

5

Feature Activation

Before feature activation, perform the system health check in Section 4.2. This check ensures that 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.

Pre-Activation Procedures

Pre-Feature Activation Health Check

Procedure 3: Perform Health Check (Pre Feature Activation)

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

 **Note:**

The Health Check procedure below is the same as the Health Check procedure described in Section 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.

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

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

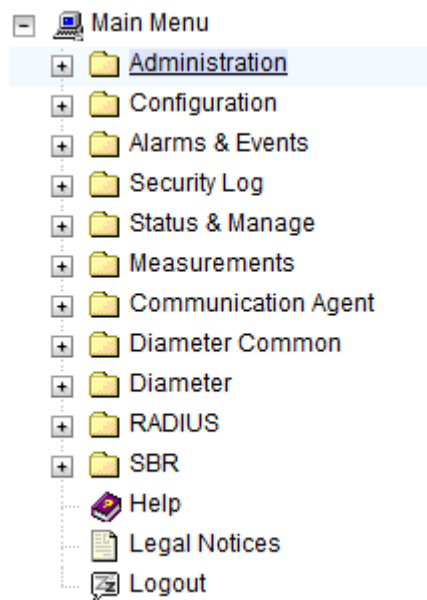
Figure 5-1 Oracle System Login



Verify if the RABR folder is not present

3. Under the **Main Menu**, verify if the RABR folder is not present.

Figure 5-2 Main Menu



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

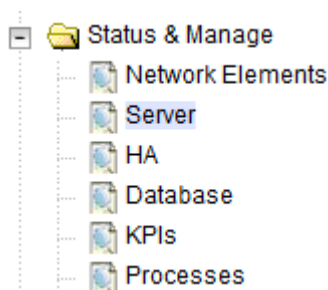
4. Open the web browser and enter the URL, `http://<Primary_NOAM_VIP_IP_Address>`
5. Log in as the `guiadmin` user.

Figure 5-3 Oracle System Login



6. Verify the server status, expand **Status & Manage** option and click **Server**

Figure 5-4 Status and Manage



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

Figure 5-5 Server Status

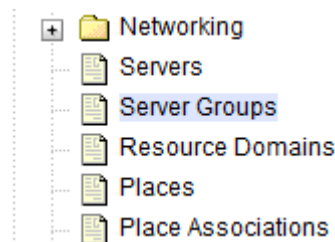
Appl State	Alm	DB	Reporting Status	Proc
Enabled	<u>Norm</u>	Norm	Norm	<u>Norm</u>
Enabled	<u>Norm</u>	Norm	Norm	Norm
Enabled	Norm	<u>Norm</u>	Norm	Norm
Enabled	Norm	Norm	Norm	<u>Norm</u>

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

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

8. Verify the Server Configuration, expand **Configuration** option and click **Server Groups**

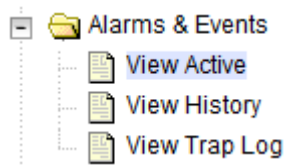
Figure 5-6 Server Groups



Verify if the configuration data is correct for your network.

9. Log current alarms, expand **Alarms & Events** option and click **View Active**

Figure 5-7 Alarms and Events



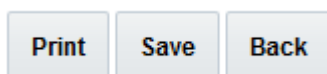
10. Click **Report**

Figure 5-8 Report



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

Figure 5-9 Save or Print



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

Activation Procedures

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

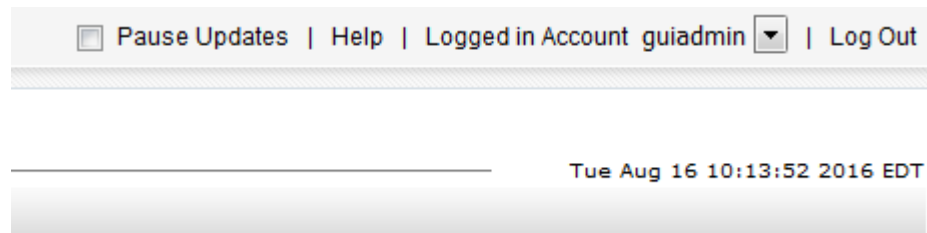
RBAR Feature Activation

Procedure 4: Feature Activation

Detailed steps for RBAR feature activation are provided in this procedure.

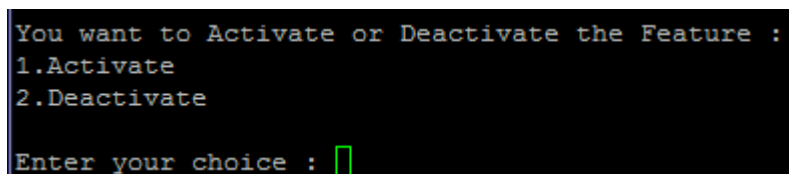
1. Log out from any active NOAM and/or SOAM GUI sessions.

Figure 5-10 Logout



2. Establish an SSH session to the NOAM VIP. Log in as `admusr`.
(Optional) Enter the result of the step here.
3. Navigate to the feature activation directory by executing the following command `$ cd /usr/TKLC/dsr/prod/maint/loaders/`
4. Execute the feature activation script, run the feature activation script by executing the following command: `$./featureActivateDeactivate`
Select **Activate**.

Figure 5-11 Activate



Select **RBAR**.

Figure 5-12 RBAR

```
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
```

Select the SOAM site for which the application will be activated:

 **Note:**

As an alternative, you can also activate on all SOAM sites.

Figure 5-13 SOAM

```
The Active SO server configured in the Topology are
=====
===
1. Jetta-SO-2
2. ALL SOs

Enter your choice on which SO you want to Activate or Deactivate the Feature : █
```

Refer to Section 7.1 for output example.

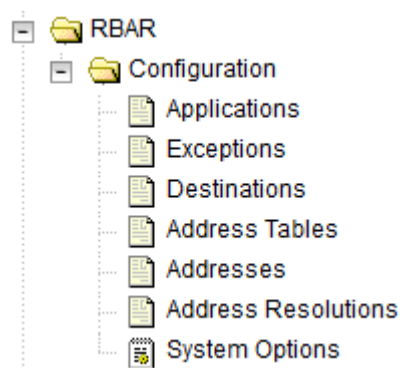
5. Establish a GUI session on the Active SOAM Server by using IP address of the SOAM server. Open the web browser and enter the following URL `http://<Active_SOAM_IP_Address>`
6. Login as the `guiadmin` user.

Figure 5-14 Oracle System Login



7. Verify if the RBAR folder is visible. Locate and verify the RBAR folder from Main Menu, check if it is visible and verify if the configuration folder items are present.

Figure 5-15 RBAR Configuration



8. Verify if the application maintenance screen is visible. Verify if the RBAR application is present in the Application Status screen. Expand the **Diameter** option, click **Maintenance** and select **Applications**.

Figure 5-16 RBAR Status

RBAR	ZombieDAM P1	Disabled	Unk	Unk	Unk	Unk
RBAR	ZombieDAM P2	Disabled	Unk	Unk	Unk	Unk

Verify if the RBAR status is uninitialized. The following data should be displayed:

- Admin State = Disabled
 - Operational Status = Unk
 - Operational Reason = Unk
 - Congestion Level = Unk
9. In the stand by SOAM GUI, repeat the verification step 5 up to step 8.

 **Note:**

If the verifications for the standby SOAM differ from the active SOAM, stop and contact My Oracle Support (MOS).

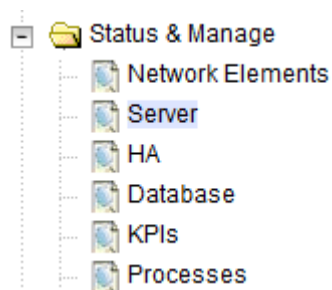
10. Establish a GUI session on the SOAM Server by using the VIP address of the SOAM server. Open the web browser and enter the URL `http://<Active_SOAM_IP_Address>`
11. Log in as the `guiadmin` user.

Figure 5-17 Oracle System Login



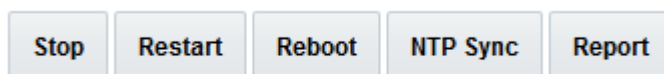
- Restart DA-MPs. Multiple iterations of this step may be executed during the feature activation procedure. This is dependent on the number of DA-MP servers within your system. Make a written record of the number of times the step was performed. It is recommended that no more than 50% of the DA-MPs be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

Figure 5-18 Server Folder



Select the desired DA-MPs, press Ctrl to select multiple DA-MPs at once.

- Click **Restart**.

Figure 5-19 Restart

Click **OK** to confirm.

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

Repeat for the additional DA-MPs.

14. Verify the RBAR application is present in the Application Status screen. Expand the **Diameter** option, click **Maintenance** and select **Applications**.

Figure 5-20 Application Status

Table Description: Applications Table

Application Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Congestion Level	Time of Last Update
RBAR	OahuMp	Disabled	Unavailable	Shut Down	Normal	2016-Sep-14 13:47:39 EDT

Verify RBAR status is initialized. The following data should display:

- Admin State = Disabled
- Operational Status = Unavailable
- Operational Reason = Shutdown
- Congestion Level = Normal

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

Post-Activation Procedures

Post-Feature Activation Health Check

Procedure 5: Perform Health Check (Post-Feature Activation)

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

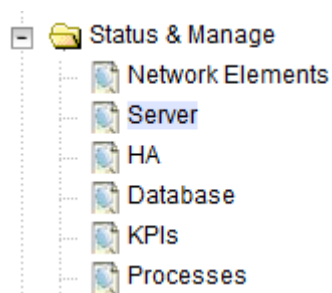
1. Log in to the NOAM VIP GUI. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter the URL `http://<Primary_NOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

Figure 5-21 Oracle System Login



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

Figure 5-22 Server Folder

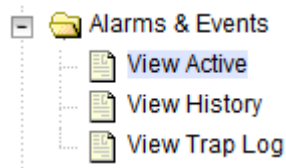


Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).

Figure 5-23 Server Status

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

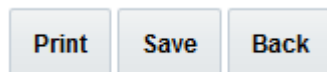
- Log current alarms. Expand **Alarms & Events** option and click **View Active**

Figure 5-24 Alarms and Events

- Click **Report**.

Figure 5-25 Report

- Click **Save** or **Print**. Keep the report copies for future reference.

Figure 5-26 Save or Print

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

6

Feature Deactivation

Execute this section only if there is a problem and it is desired to revert back to the pre-activation version of the software. In general, as long as there are no Application Routing Rules using the RBAR application, it will have no impact on the system and does not need to be deactivated. The deactivation procedure will cause all the RBAR related configuration data to be removed. The crafts person must ensure that this is acceptable.

Pre-Deactivation Procedures

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

Pre-Feature Deactivation Health Check

Procedure 6: Perform Health Check (Pre-Feature Deactivation)

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

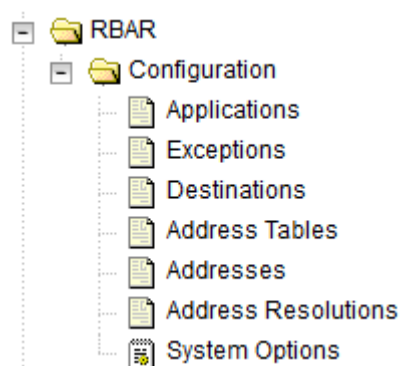
1. Log in to the SOAM VIP GUI. Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter the URL `http://<Primary_SOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user

Figure 6-1 Oracle Systemn Login



3. In the SOAM VIP GUI, verify if the RBAR folder is visible. Locate and verify if the RBAR folder from Main Menu is visible and the configuration folder items are present.

Figure 6-2 RBAR Configuration Folder



 **Note:**

It should only be present after feature activation, so if it is not present, then the feature is already deactivated and there is no need to complete this deactivation procedure.

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

Figure 6-3 Oracle System Login



ORACLE®

Oracle System Login Mon Jul 11 13:59:37 2016 EDT

Log In
Enter your username and password to log in

Username:

Password:

Change password

Welcome to the Oracle System Login.

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

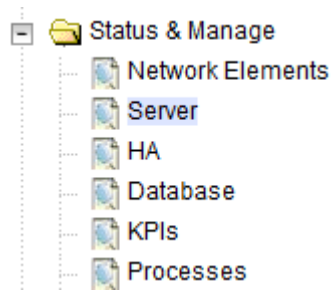
Unauthorized access is prohibited.

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

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

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

Figure 6-4 Server Folder



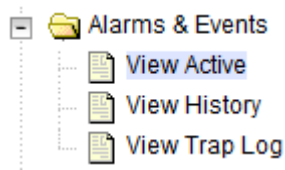
7. Verify if all Server Status is Normal (Norm) for, Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).

Figure 6-5 Server Status

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

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

Figure 6-6 Alarms and Events



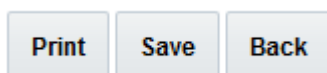
9. Click **Report**.

Figure 6-7 Report



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

Figure 6-8 Save or Print



Compare this alarm report with those gathered in the pre-activation procedures.

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

Deactivation Procedures

RBAR Feature Deactivation

Procedure 7: Feature Deactivation

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

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

Figure 6-9 Oracle System Login

ORACLE®

Oracle System Login Mon Jul 11 13:59:37 2016 EDT

Log In

Enter your username and password to log in

Username:

Password:

Change password

Welcome to the Oracle System Login.

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

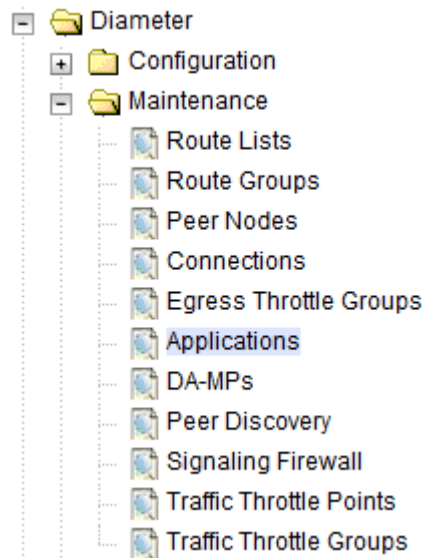
Unauthorized access is prohibited.

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

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

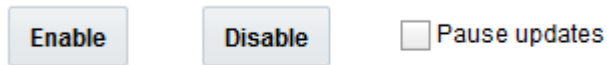
3. Disable RBAR application, expand the **Diameter** option, click **Maintenance** and select **Applications**.

Figure 6-10 RBAR Applications



4. Select the RBAR applications to disable and click **Disable**.

Figure 6-11 Disable



5. Click **OK** to confirm.

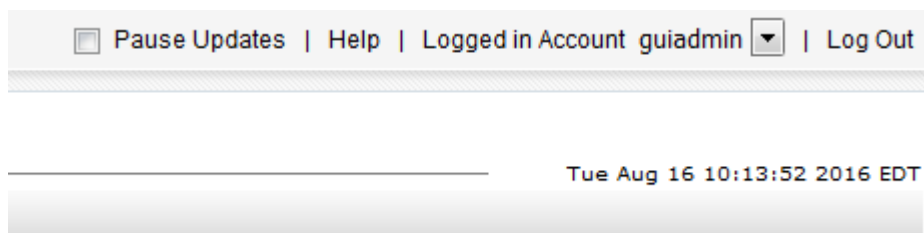
Figure 6-12 Shut Down

Table Description: Applications Table

Application Name	MP Server Hostname	Admin State	Operational Status	Operational Reason	Congestion Level	Time of Last Update
RBAR	OahuMP	Disabled	Unavailable	Shut Down	Normal	2016-Sep-14 13:47:39 EDT

6. Log out of any active NOAM and/or SOAM GUI sessions.

Figure 6-13 Logout



7. Establish a SSH session to the NOAM VIP. Log in as `admusr`.

8. Navigate to the feature activation directory by executing the command `$ cd /usr/TKLC/dsr/prod/maint/loaders/`
9. In the NOAM VIP GUI, run the feature activation script by executing the following command: `$./featureActivateDeactivate`

Select **Deactivate**.

Figure 6-14 Deactivate

```
You want to Activate or Deactivate the Feature :
1.Activate
2.Deactivate
Enter your choice : █
```

Select **RBAR**.

Figure 6-15 RBAR Feature

```
Which Feature you want to DeActivate :
1.RBAR
2.FABR
3.Mediation
4.LoadGen
5.GLA
6.MAP Interworking
7.DTLS
8.DCA Framework
9.DCA Application
```

Select the SOAM site for which the application will be deactivated:

 **Note:**

As an alternative, you can also deactivate on all SOAM sites:

Figure 6-16 Feature Deactivation

```
The Active SO server configured in the Topology are
=====
===
1. Jetta-SO-2
2. ALL SOs
Enter your choice on which SO you want to Activate or Deactivate the Feature : █
```

Refer to Section 7.2 for output example.

10. Log in to the active SOAM GUI, establish a GUI session on the active SOAM server by using IP address of the SOAM server. Open the web browser and enter the URL `http://<Active_SOAM_IP_Address>`
11. Login as the `guiadmin` user.

Figure 6-17 Oracle System Login



12. In the active SOAM GUI, verify if the RBAR folder is not visible under Main Menu.
13. Repeat Step 10-12 for the standby SOAM.

 **Note:**

If the verifications for the standby SOAM differ from the active SOAM, stop and contact My Oracle Support (MOS).

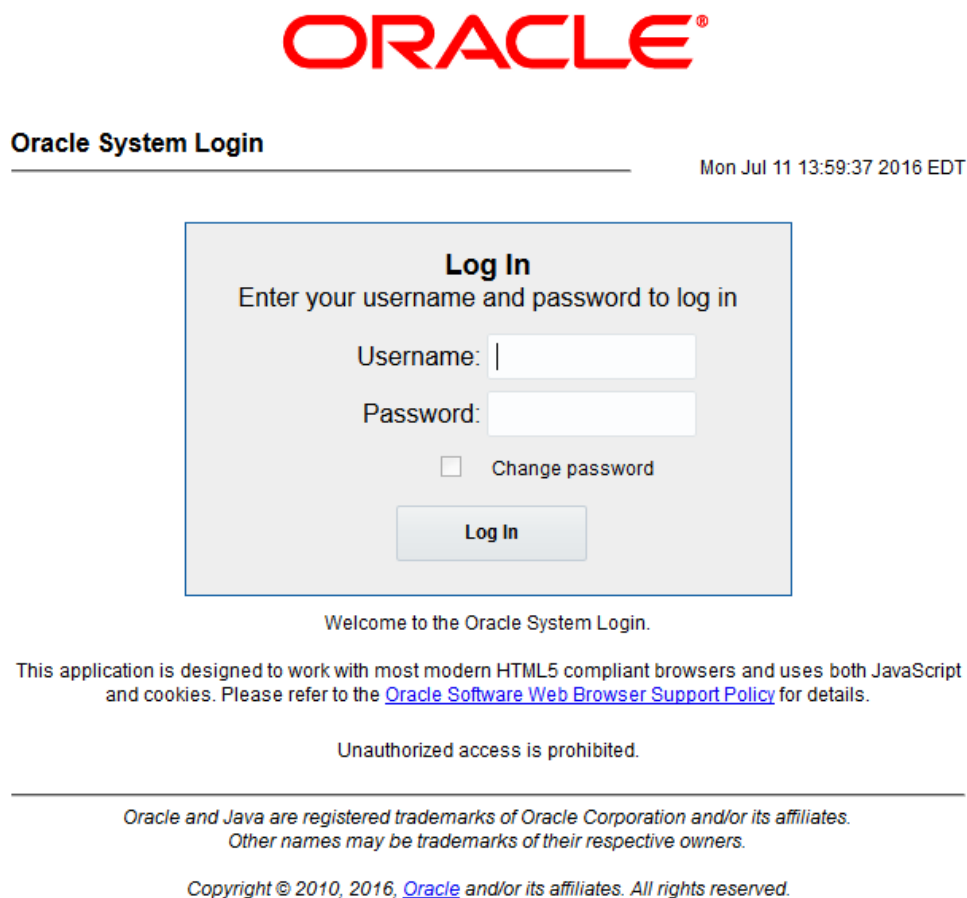
14. Repeat steps 10-12 for any spare SOAMs present.

 **Note:**

If the verifications for the standby SOAM differ from the active SOAM, stop and contact My Oracle Support (MOS).

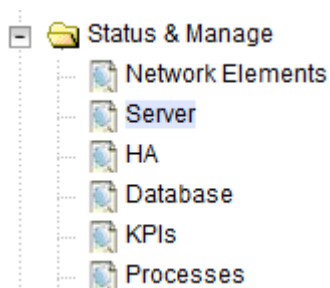
15. Login to the SOAM VIP GUI. Establish a GUI session on the SOAM server by using the VIP address of the SOAM server. Open the web browser and enter the URL `http://<Primary_SOAM_VIP_IP_Address>`.
16. Log in as the `guiadmin` user.

Figure 6-18 Oracle System Login



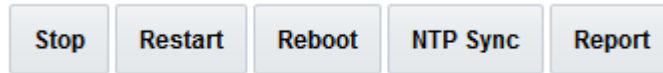
17. In the SOAM VIP GUI, restart the DA-MPs. Multiple iterations of this step may be executed during the feature deactivation procedure. This is dependent on the number of DA-MP servers within your system. Make a written record of the number of times the step was performed. It is recommended that no more than 50% of the DA-MPs be restarted at once. Expand **Status & Manage** option and click **Server**.

Figure 6-19 Server Folder



18. Select the desired DA-MPs, press **Ctrl** to select multiple DA-MPs at once. Click **Restart**.

Figure 6-20 Restart



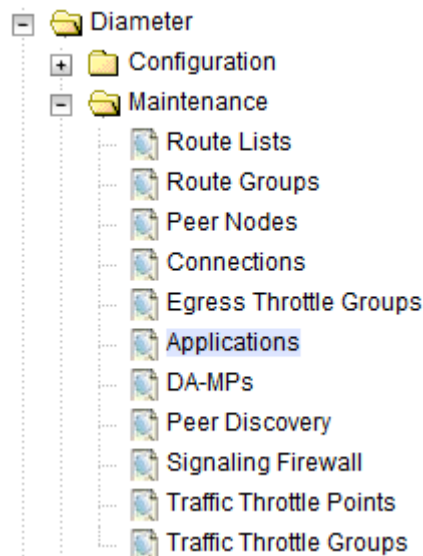
Click **OK** to confirm.

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

Repeat for the additional DA-MPs.

19. In the SOAM VIP GUI, verify the maintenance screen. Expand the **Diameter** option, click **Maintenance** and select **Applications**.

Figure 6-21 Applications Folder



Verify if the RBAR application is not present.

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

Post-Deactivation Procedures

To complete a deactivation, complete the Post-Deactivation by following the procedures in this chapter.

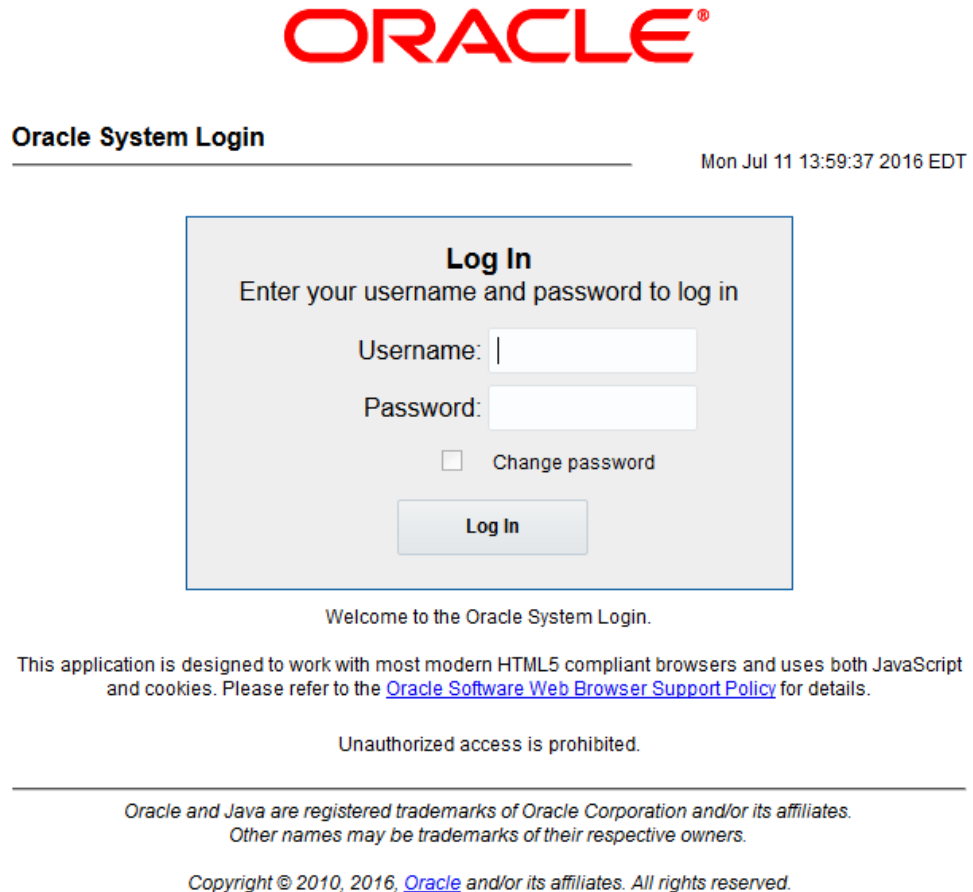
Post-Feature Deactivation Health Check

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

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

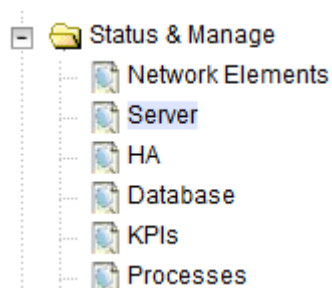
1. Log in to the NOAM VIP GUI. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter the URL `http://<Primary_NOAM_VIP_IP_Address>`
2. Log in as the `guiadmin` user.

Figure 6-22 Oracle System Login



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

Figure 6-23 Server Folder



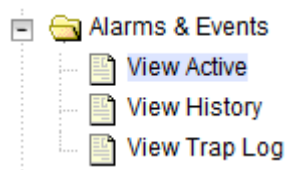
Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).

Figure 6-24 Server Status

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

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

Figure 6-25 Alarms and Events



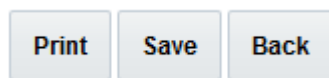
5. Click **Report**.

Figure 6-26 Report



6. Click **Save** or **Print**. Keep the report copies for future reference.

Figure 6-27 Save or Print



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

7

Engineering Notes

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

Sample Output of Activation (Active NOAM)

Run script to activate RBAR feature:

```
=====S-T-A-R-
T=====
Engineering
=====
=====
Execution of Activation/Deactivation Process Starts
=====
=====
Starting Activation/Deactivation process....
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.rbarActivateAsourced script on N01
=====
===
Add RBAR KPI group
=====
===
KPI_Group=RBAR
Visibility=VIS_SO
=====
===
Add RBAR Measurement groups
=====
===
Meas_Group=Address Resolution Performance
Visibility=VIS_SO
=====
Meas_Group=Address Resolution Exception
Visibility=VIS_SO
=====
===
Add RBAR GUI Configuration Permissions.
=====
===
_appid=17
group_id=7000
group_name=RBAR Configuration Permissions
=====
=====
```

```
Starting to Execute the Loaders on Mate server
=====
=====
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.rbarActivateAsourced script on NO2
=====
=====
FIPS integrity verification test failed.
KPI_Group=RBAR
Visibility=VIS_SO
=====
Meas_Group=Address Resolution Performance
Visibility=VIS_SO
=====
Meas_Group=Address Resolution Exception
Visibility=VIS_SO
=====
=====
Add RBAR GUI Configuration Permissions.
=====
=====
_appid=17group_id=7000group_name=RBAR Configuration Permissions
=====
FIPS integrity verification test failed.
=====
=====
The Active SO server configured in the Topology are
=====
=====
1. SO1
2. ALL SOs
Enter your choice on which SO you want to Activate or Deactivate the
Feature :1
=====
=====
This is a 3 Tier Setup , So run the B sourced loaders on SO server :
SO1
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.rbarActivateBsourced script on SO1
FIPS integrity verification test failed.
=====
=====
Current server is HA ACTIVE
=====
=====
Add RBAR to DsrApplication. If already present, do not update -
display awarning instead
=====
=====
Verify that RBAR is in the table
=====
=====
id=3
name=RBAR
unavailableAction=ContinueRouting
```

```
avpInsertion=Yes
shutdownMode=Forced
shutdownTimer=0
resultCode=3002
vendorId=0
errorString=RBAR Unavailable
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=RBAR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
=====
===
Add Common DSR Application measurements for RBAR.
=====
===
repgrp=DSR Application Exception
measid=10302
subgrp=
=====
repgrp=DSR Application Exception
measid=10303
subgrp=
=====
repgrp=DSR Application Performance
measid=10300
subgrp=
=====
repgrp=DSR Application Performance
measid=10301
subgrp=
=====
repgrp=DSR Application Performance
measid=10304
subgrp=
=====
repgrp=DSR Application Performance
measid=10305
subgrp=
=====
repgrp=DSR Application Performance
measid=10350
subgrp=
=====
===
Add RBAR GUI Configuration Permissions.
=====
===
_appid=17
group_id=7000
group_name=RBAR Configuration Permissions
=====
FIPS integrity verification test failed.
```



```
=====
=====
Executing the Loaders and Clearing Cache on Standby SO servers.
=====
=====
Starting to Execute the Loaders on Mate server
=====
=====
Executing /usr/TKLC/dsr/prod/maint/loaders/activate/
load.rbarActivateB sourced script on SO2
=====
=====
FIPS integrity verification test failed.
=====
=====
Current server is HA STANDBY
=====
=====
Verify that RBAR is in the table
=====
=====
id=3
name=RBAR
unavailableAction=ContinueRouting
avpInsertion=Yes
shutdownMode=Forced
shutdownTimer=0
resultCode=3002
vendorId=0
errorString=RBAR Unavailable
resExhResultCode=3004
resExhVendorId=0
resExhErrorString=RBAR Resource Exhausted
routeListId=-1
realm=
fqdn=
mcl=0
=====
=====
Add Common DSR Application measurements for RBAR.
=====
=====
repgrp=DSR Application Exception
measid=10302
subgrp=
=====
repgrp=DSR Application Exception
measid=10303
subgrp=
=====
repgrp=DSR Application Performance
measid=10300
subgrp=
=====
repgrp=DSR Application Performance
```

```
measid=10301
subgrp=
=====
repgrp=DSR Application Performance
measid=10304
subgrp=
=====
repgrp=DSR Application Performance
measid=10305
subgrp=
=====
repgrp=DSR Application Performance
measid=10350
subgrp=
=====
===
Add RBAR GUI Configuration Permissions.
=====
===
_appid=17
group_id=7000
group_name=RBAR Configuration Permissions
=====
FIPS integrity verification test failed.
=====
=====
Do you want to activate/deactivate this feature on another System OAM
Server[Y/N] :
n
[admusr@NO1 loaders]$
```

Sample Output of De-Activation (Active NOAM)

Run script to deactivate RBAR 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. SO1
2. ALL SOs

Enter your choice on which SO you want to Activate or Deactivate the
Feature :1
Verifying feature is activated or not on SO1FIPS integrity verification test
```

```
failed.
=====
RBAR is activated on S01
=====
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/
load.rbarDeactivateAsourced script on N01
    === deleted 1 records ===
    === deleted 1 records ===
    === deleted 1 records ===
=====
=====
Removing RBAR GUI permissions.
=====
=====
    === deleted 1 records ===
=====
=====
Starting to Execute the Loaders on Mate server
=====
=====
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/
load.rbarDeactivateAsourced script on N02
=====
=====
FIPS integrity verification test failed.
=====
=====
Removing RBAR GUI permissions.
=====
=====
    === deleted 1 records ===
FIPS integrity verification test failed.
=====
=====
This is a 3 Tier Setup , So run the B sourced loaders on SO server :
S01
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/
load.rbarDeactivateBsourced script on S01
FIPS integrity verification test failed.
=====
=====
Current server is HA ACTIVE
=====
=====
    === deleted 0 records ===
=====
=====
Verify there are no dsrAppId=3 [RBAR] entries
=====
=====
    id priority                                name
action
ansResultCode
errorMessage
vendorId   dsrAppId appRouteTableId gxPrimeRequest
```

```

birthTime
mcl
  0      1          Gx_ART_Rule
RouteToAppl
0
0
6          1          No 05/18/2015 16:28:13.000          27
=== deleted 2 records ===
=====
===
Verify dsrAppId=3 [RBAR] are not present in the DsrApplicationPerMp table
=====
===
=== deleted 1 records ===
=====
===
Verify RBAR is not present in the DsrApplication table
=====
===
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=====
===
Removing RBAR GUI permissions.
=====
===
=== deleted 1 records ===
FIPS integrity verification test failed.
=====
=====
Executing the Loaders and Clearing Cache on Standby SO servers.
=====
=====
Starting to Execute the Loaders on Mate server
=====
=====
Executing /usr/TKLC/dsr/prod/maint/loaders/deactivate/
load.rbarDeactivateB sourced script on S02
=====
=====
FIPS integrity verification test failed.
=====
===
Current server is HA STANDBY
=====
===
Verify there are no dsrAppId=3 [RBAR] entries
=====
===
id priority          name          action

```

```
ansResultCode
errorMessage
vendorId   dsrAppId appRouteTableId gxPrimeRequest
birthTime
mcl
      0          1                      Gx_ART_Rule
RouteToAppl
0
      0
6          1                      No 05/18/2015
16:28:13.000                27
=====
=====
Verify dsrAppId=3 [RBAR] are not present in the DsrApplicationPerMp
table
=====
=====
Verify RBAR is not present in the DsrApplication table
=====
=====
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=== deleted 1 records ===
=====
=====
Removing RBAR GUI permissions.
=====
=====
=== deleted 1 records ===
FIPS integrity verification test failed.
=====
=====
Do you want to activate/deactivate this feature on another System OAM
Server[Y/N] :
      n
```

A

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.

B

Locate Product Documentation on the Oracle Help Center Site

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.