Oracle® Communications

Diameter Signaling Router

DSR API Gateway Disaster Recovery Guide

Release 8.3

E93228-01

September 2018

ORACLE

Oracle® Communications Diameter Signaling Router, DSR API Gateway Disaster Recovery Guide, Release 8.3

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

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

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

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

See more information on My Oracle Support (MOS).

Table of Contents

List of Tables

List of Figures

List of Procedures

1. Introduction

1.1 Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for DSR API Gateway. This includes recovery of partial or a complete loss of one or more DSR APIGW servers. The audience for this document includes GPS groups such as Software Engineering, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. This document can also be executed by Oracle customers, as long as Oracle Customer Service personnel are involved and/or consulted. This document provides step-by-step instructions to execute disaster recovery for DSR APIGW. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note: Failures can happen from the host or Infrastructure level too. Different infrastructures have different approaches to recover VMs which is not covered in this document. For example, VMWare has a vMotion feature which can migrate VM from one host to another. Any such Infrastructure/Hypervisor related migrations/disaster recovery scenarios are out of scope of this document. This document covers the DR scenarios within the DSR application.

1.2 References

[1] DSR API Gateway Installation Guide

[2] DSR/SDS NOAM Failover User's Guide

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1: Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DSR	Diameter Signaling Router
ESXi	Elastic Sky X Integrated
FABR	Full Address Based Resolution
GW	Gateway
iDIH	Integrated Diameter Intelligence Hub
IPFE	IP Front End
IWF	Inter Working Function
NAPD	Network Architecture Planning Diagram
NOAM	Network Operations, Administration & Maintenance
OS	Operating System
OVA	Open Virtualization Appliance
PDRA	Policy Diameter Routing Agent
PCA	Policy and Charging Application

Acronym	Definition
RBAR	Range Based Address Resolution
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution
VM	Virtual Machine
vSTP	Virtual Signaling Transfer Point

1.4 Terminology

This section describes terminology as it is used within this document.

Table 2: Terminology

Term	Definition
Base software	Base software includes deploying the VM image.
Failed server	A failed server in disaster recovery context refers to a VM that has suffered partial or complete software failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software.
Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware or hardware firmware, and is not responsible for hardware installation, configuration, or maintenance.
Enablement	The business practice of providing support services (hardware, software, documentation, etc.) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.

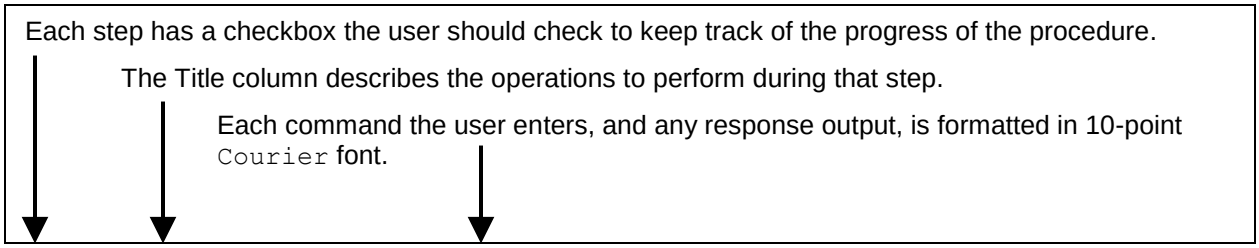
1.5 How to Use this Document

When executing the procedures in this document, there are a few key points that help ensure the user understands procedure convention. These points are:

1. Before beginning a procedure, completely read the instructional text (it displays immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
2. Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.
3. If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact My Oracle Support (MOS) for assistance, as described in Appendix D before attempting to continue.

Figure 1 shows an example of a procedural step used in this document.

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 and step 2 and substep 2.1.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.



	Title/Instructions	Directive/Result Steps
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	Verify Network Element data	1. View the Network Elements configuration data; verify the data; save and print report. 2. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example Procedure Steps Used in This Document

1.6 General Description

The DSR APIGW disaster recovery procedure falls into following categories:

Recovery of the entire network from a total outage [Recovery Scenario 1: Complete Database Server Outage]	All Database servers failed
Recovery with one database server intact [Recovery Scenario 2: Partial Server Outage with One Database Server Intact]	One database servers intact
Recovery with Application servers lost [Recovery Scenario 1: Admin Server is Up and Running, and Application Server(s) is Lost]	All application servers failed
Recovery of Admin server [Recovery Scenario 2:]	Admin server failed
Recovery of Admin and lost Application servers [Recovery Scenario 3:]	• Admin server failed • One application server intact
Recover of both Admin and Application servers [Recovery Scenario 4: Admin and Application Servers are Lost]	Both admin and application server failed

2. Procedure Overview

This section lists the materials required to perform disaster recovery procedures and a general overview (disaster recovery strategy) of the procedure executed.

2.1 Required Materials

The following items are needed for disaster recovery:

- A hard copy of this document and hard copies of all documents in the reference list.
- Hard copy of all NAPD performed at the initial installation and network configuration of this site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
- DSR APIGW recent backup files: electronic backup file (preferred) or hard copy of all DSR APIGW configuration and provisioning data.
- Latest network interface data; XSI interface lost
- The **ocsgdr.praperties** file to fill-in the parameter details.
- **recoverAdminServer.py** script to recover admin server.
- **recoverAppServers.py** script to recover application server.

2.2 Procedure Preparation

Disaster recovery procedure execution is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. Use Table 3: Recovery Scenarios to evaluate the correct recovery scenario and follow the procedure(s) listed to restore operations.

Note: A failed server in disaster recovery context refers to a server that has suffered partial or complete software failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-deploy base software.

Table 3: Recovery Scenarios

Recovery Scenario	Failure Condition	Section
1	All database servers failed	Section Recovery Scenario 1: Complete Database Server Outage
2	At least one database server is intact and available	Section Recovery Scenario 2: Partial Server Outage with One Database Server Intact
3	Admin server is up and running, and application server(s) is lost	Section Recovery Scenario 1: Admin Server is Up and Running, and Application Server(s) is Lost
4	Application servers are up and running, and admin server is lost	Section Recovery Scenario 2:
5	At least one application server is up, and admin and application servers are lost	Section Recovery Scenario 3: At Least One Application Server is Up, and Admin and Applications Servers are Lost
6	Admin and application servers are lost	Section Recovery Scenario 4: Admin and Application Servers are Lost

3. DSR APIGW Database Disaster Recovery Procedure

Call My Oracle Support (MOS) before executing this procedure to ensure the proper recovery planning is performed.

Before disaster recovery, users must properly evaluate the outage scenario. This check ensures the correct procedures are executed for the recovery.

!!WARNING!!

Note: Disaster recovery is an exercise that requires collaboration of multiple groups and is expected to be coordinated by the Oracle support prime. Based on Oracle support's assessment of disaster, it may be necessary to deviate from the documented process.

3.1 Recovering and Restoring System Configuration

Disaster recovery requires configuring the system as it was before the disaster and restoration of operational information.

!!WARNING!!

Whenever there is need to restore the backup for database servers in any of recovery scenarios described in the following sections, the backup directory may not be available in the system as system since the system is DRed. In this case, refer to Appendix B Workarounds for steps to check to create the backup directory.

File format for recovery is when the backup was taken. Generally, the backup file is in this format:

Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

3.1.1 Recovery Scenario 1: Complete Database Server Outage

For a complete server outage, DSR APIGW database servers are recovered using recovery procedures for software and then executing a database restore to the active DSR APIGW database (DB1) server. All other servers are recovered using recovery procedures for software.

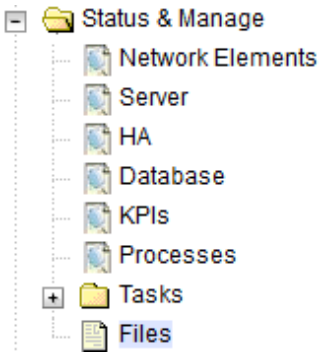
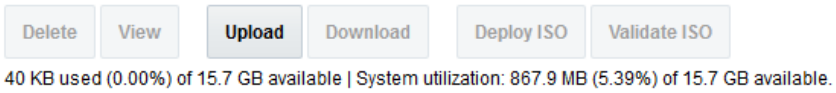
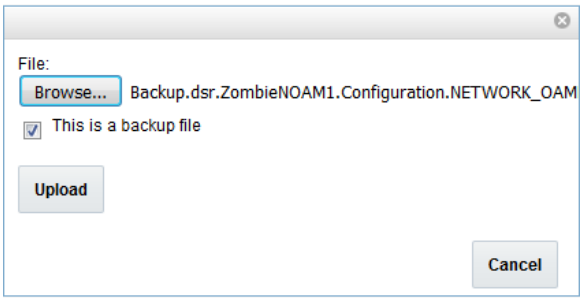
Database replication from the active DSR APIGW database (DB1) server recovers the database on these servers. The major activities are summarized as follows:

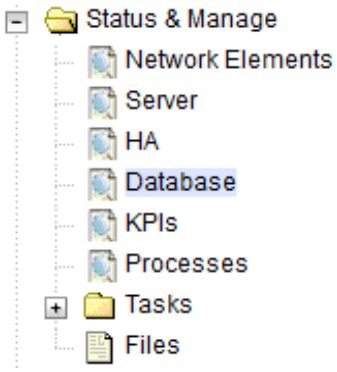
- Recover base software for all VMs:
  - Recover the virtual machines hosting the DSR APIGW database.
  - Recover the **active DSR APIGW database (DB1)** server by recovering the NOAMs base software.
  - Recover the DSR APIGW database.
  - Reconfigure the application.
- Recover the **standby DSR APIGW database** (DB2) server by recovering base software, for a non-HA deployment this can be skipped.
  - Reconfigure the DSR application.
- Restart process and re-enable provisioning replication.

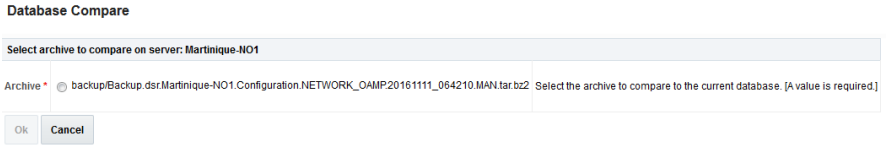
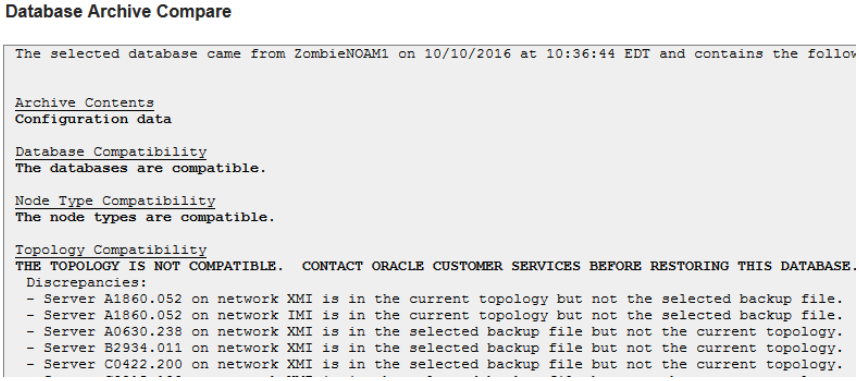
Procedure 1. Recovery Scenario 1

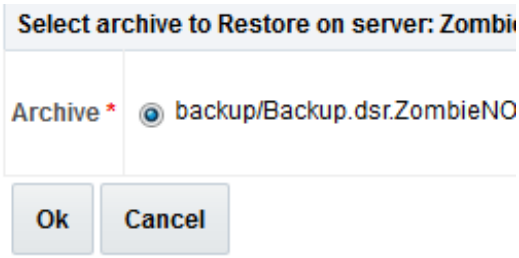
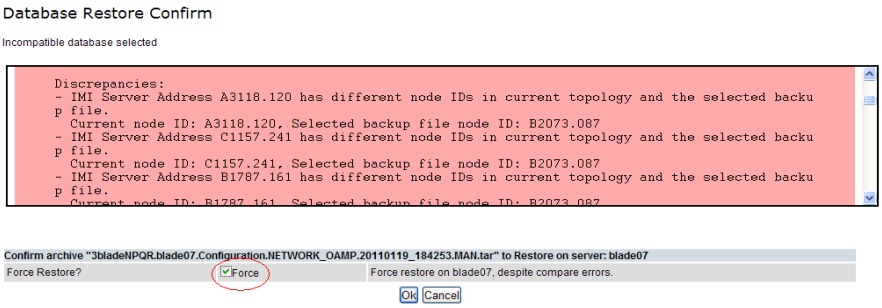
Step #	Procedure	Description
This procedure recovers servers if both DSR APIGW database servers are failed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	Workarounds	Refer to Appendix B Workarounds to understand/apply any workarounds required during this procedure.
2. ☐	Gather required materials	Gather the documents and required materials listed in Section Required Materials.
3. ☐	Recover the failed software	**For VMWare based deployments**: 1. For DSR APIGW database servers, execute the following procedures from reference [1]: a. Import DSR APIGW Database and Admin/Application OVAs (VMware). ***Note:*** If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Create DSR APIGW Database VMs (VMware). **For KVM/OpenStack based deployments**: 1. For DSR APIGW database servers, execute the following procedures from reference [1]: a. Import DSR APIGW Database and Admin/Application OVAs (OpenStack) ***Note:*** If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Create DSR APIGW Database VMs (OpenStack).
4. ☐	Obtain latest database backup and network configuration data	1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources. 2. From required materials list in the Required Materials section, use the site survey documents and Network Element report (if available) to determine network configuration data.
5. ☐	Execute DSR APIGW installation procedure for the database (DB1) server	1. Verify the networking data for network elements. ***Note:*** Use the backup copy of network configuration data and site surveys (step 2). 2. Execute installation procedures for the database (DB1) server from reference [1] Configure DSR APIGW Database.

Step #	Procedure	Description
6. ☐	**DSR APIGW Database GUI**: Login	Log into the database (DB1) GUI as the **guiadmin** user: 

Step #	Procedure	Description
7. ☐	**DSR APIGW Database GUI**: Upload the backup database file	1. Navigate to **Status and Manage > Files**.  2. Select the active **DSR APIGW Database (DB1)** server. 3. Click **Upload** and select the **NO Provisioning and Configuration** file backed up after initial installation and provisioning.  4. Click **Browse** and locate the backup file. 5. Mark the **This is a backup file** checkbox. 6. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

Step #	Procedure	Description
8. ☐	**DSR APIGW Database GUI**: Disable provisioning	1. Navigate to **Status and Manage > Database**.  2. Disable Provisioning by clicking **Disable Provisioning** at the bottom of the screen. 3. Click **OK** to confirm.  The **Warning Code 002** displays.

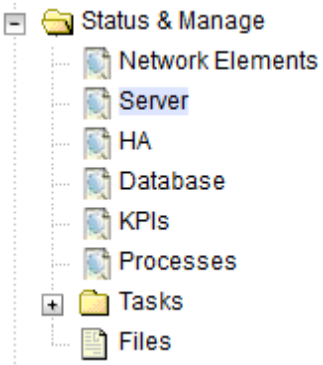
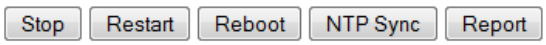
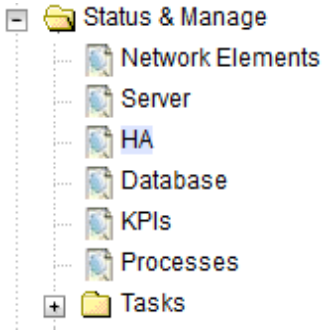
Step #	Procedure	Description
9. ☐	**DSR APIGW Database GUI**: Verify the archive contents and database compatibility	1. Select the **Active DSR APIGW Database** server and click **Compare**. 2. Click the button to restore the database file uploaded in step 7.  3. Verify the output window matches the screen shown here.  ***Notes***: • You will get a database mismatch regarding the Node IDs of the VMs that is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix D: My Oracle Support (MOS). • Archive contents and database compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. • The following is expected output for the Topology Compatibility Check since we are restoring from existing backed up database to database with just one DSR APIGW Database. **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. We are trying to restore a backed up database into an empty NOAM database. This is an expected text in topology compatibility. 4. If the verification is successful, click **Back** and continue to next step in this procedure.

Step #	Procedure	Description
10. ☐	**Active DSR APIGW Database**: Restore the database	1. Navigate to **Status and Manage > Database**. 2. Select the **Active DSR APIGW Database** server and click **Restore**. 3. Select the backup provisioning and configuration file. 4. Click **OK**.  ***Note:*** A database mismatch regarding the NodeIDs of the servers is expected. If that is the only mismatch, proceed; otherwise, stop and contact My Oracle Support (MOS). 5. Mark the **Force** checkbox and click **OK** to proceed with the DB restore.  ***Note:*** After the restore has started, the user is logged out of XMI NO GUI since the restored topology is old data.

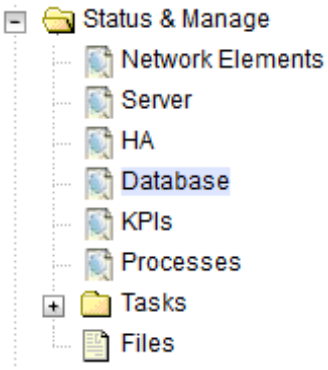
Step #	Procedure	Description
11. ☐	**DSR APIGW Database VIP GUI**: Login	1. Establish a GUI session on the DSR APIGW database server by using the VIP IP address of the DSR APIGW database server. Open the web browser and enter a URL of: `http://<Primary_ DSR APIGW Database_VIP_IP_Address>` 2. Login as the **guiadmin** user. 
12. ☐	**DSR APIGW Database VIP GUI**: Monitor and confirm database restoral	Wait for **5-10 minutes** for the system to stabilize with the new topology: Monitor the Info tab for **Success**. This indicates the backup is complete and the system is stabilized. The following alarms **must** be ignored for NOAM and MP servers until all the servers are configured: Alarms with Type Column as **REPL** , **COLL**, **HA** (with mate NOAM), **DB** (about Provisioning Manually Disabled). ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The configuration and maintenance information is in the same state it was when backed up during initial backup.
13. ☐	**DSR APIGW Database NOAM**: Login	Log into the recovered active DSR APIGW database using the SSH terminal as **admusr** user.

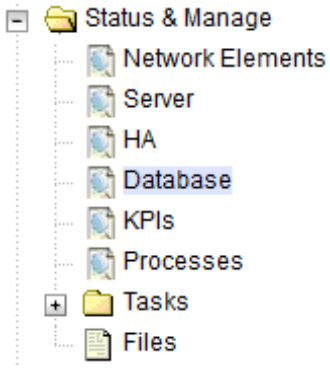
Step #	Procedure	Description
14. ☐	**DSR APIGW Database VIP GUI**: Recover standby DSR APIGW database (DB2)	Install the second DSR APIGW database server by executing procedures from reference [1] Configure DSR APIGW Database.

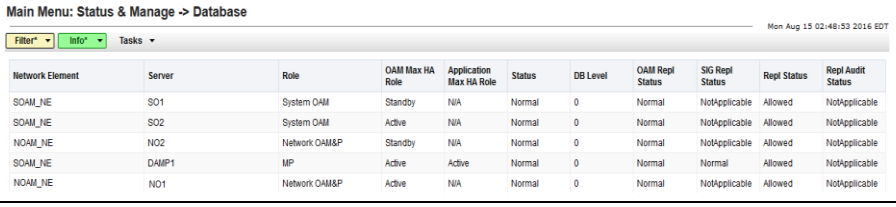
15. ☐	**Active DSR APIGW Database (DB1)**: Correct the RecognizedAuthority table	1. Establish an SSH session to the active DSR APIGW database and login as **admusr**.
		2. Execute this command:
		`$ sudo top.setPrimary`
		`- Using my cluster: A1789`
		`- New Primary Timestamp: 11/09/15 20:21:43.418`
		`- Updating A1789.022: <DSR_NOAM_B_hostname>`
		`- Updating A1789.144: <DSR_NOAM_A_hostname>`

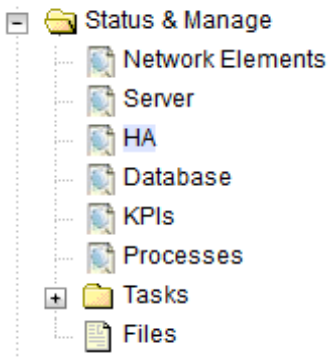
16. ☐	**DSR APIGW Database VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby DSR APIGW database server and click **Restart**. 
17. ☐	**DSR APIGW Database VIP GUI**: Set HA on standby DSR APIGW database	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the standby DSR APIGW database server and set it to **Active**. 4. Click **OK**.

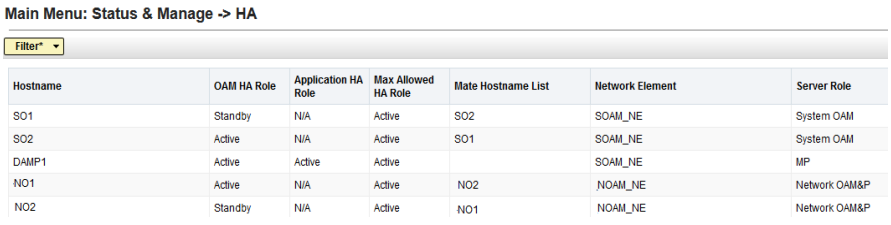
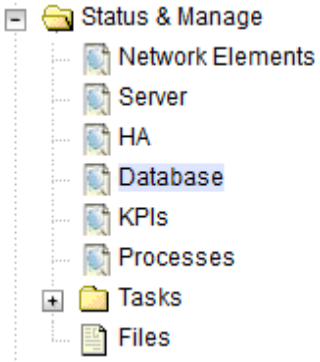
Step #	Procedure	Description

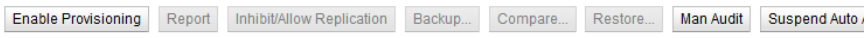
18. ☐	**DSR APIGW Database VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.
		 
		2. Select the active DSR APIGW database server and click **Report**.
		The following screen displays.
		Main Menu: Status & Manage -> Database [Report]
		`dsr Database Status Report`
		`Report Generated: Tue Oct 11 13:24:26 2016 EDT`
		`From: Active Network OAM&P on host ZombieNOAM1`
		`Report Version: 8.0.0.0.0-80.9.0`
		`User: guiadmin`
		`General`
		`Hostname : ZombieNOAM1`
		`Database Birthday : 2016-07-11 11:21:50 EDT`
		`Appworks Database Version : 6.0`
		`Application Database Version :`
		`Capacities and Utilization`
		`Disk Utilization 8.4%: 585M used of 7.0G total, 6.0G available`
		`Memory Utilization 0.0%: used of total, 0M available`
		3. Click **Save** and save the report to your local machine.

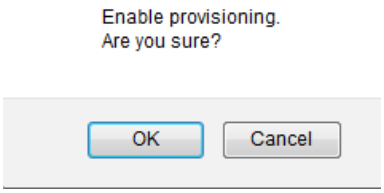
<table>
<tr><th>Step #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>19.
☐</td><td>Active DSR APIGW Database: Verify replication between servers</td><td>1. Log into the active DSR APIGW database using the SSH terminal as admusr user.
2. Execute this command:
<pre>$ sudo irepstat -m</pre>Output like below shall be generated:<pre>-- Policy 0 ActStb [DbReplication] ------------------------------
RDU06-MP1 -- Stby
  BC From RDU06-SO1 Active 0 0.50 ^0.17%cpu 42B/s A=none
  CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none
RDU06-MP2 -- Active
  BC From RDU06-SO1 Active 0 0.50 ^0.10%cpu 33B/s A=none
  CC To   RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none
RDU06-NO1 -- Active
  AB To   RDU06-SO1 Active 0 0.50 1%R 0.03%cpu 21B/s
RDU06-SO1 -- Active
  AB From RDU06-NO1 Active 0 0.50 ^0.04%cpu 24B/s
  BC To   RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s
  BC To   RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s</pre></td></tr>
<tr><td>20.
☐</td><td>DSR APIGW Database VIP GUI: Verify the database states</td><td>1. Navigate to Status and Manager > Database.
 

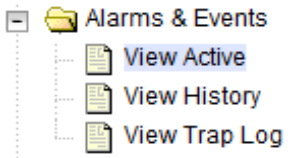
2. Verify the OAM Max HA Role is either Active or Standby for DSR APIGW database and the status is Normal.
 
</td></tr>
</table>

<table>
<tr><th>Step #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>21.
☐</td><td>DSR APIGW Database VIP GUI: Verify the HA status</td><td>1. Navigate to Status and Manage > HA.
 

2. Select the row for all of the servers.
3. Verify the HA Role is either Active or Standby.
 
</td></tr>
<tr><td>22.
☐</td><td>DSR APIGW Database GUI: Enable provisioning</td><td>1. Navigate to Status and Manage > Database.
 

2. Click Enable Provisioning.
 

3. Click OK to confirm.
 
</td></tr>
</table>

Step #	Procedure	Description
23. ☐	**DSR APIGW Database VIP GUI**: Examine all alarms	1. Log into the DSR APIGW database VIP, if not already logged in. 2. Navigate to **Alarms and Events > View Active**.  3. Examine all active alarms and refer to the on-line help for how to address them. 4. If needed, contact My Oracle Support (MOS).
24. ☐	Back up and archive all the databases from the recovered system	Execute Appendix A DSR Database Backup.

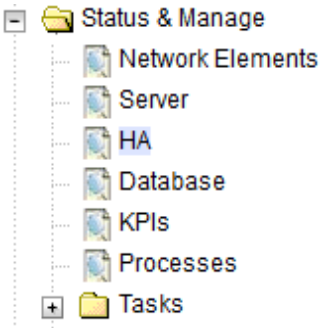
3.1.2 Recovery Scenario 2: Partial Server Outage with One Database Server Intact

This procedure covers a partial server outage with a DSR APIGW database server intact and available. All other servers are recovered using recovery procedures for software. Database replication from the active NOAM server recovers the database on these servers. The major activities are summarized as follows:

- Recover standby DSR APIGW database server (if needed) by recovering software and the database.
  - Recover the software.

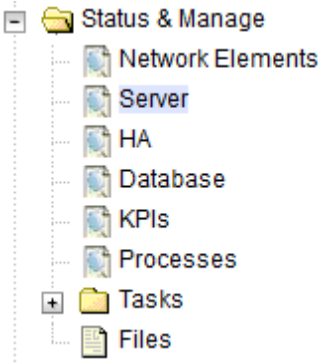
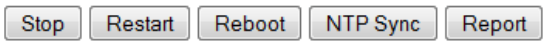
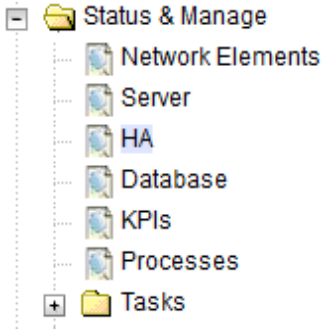
Procedure 2. Recovery Scenario 2

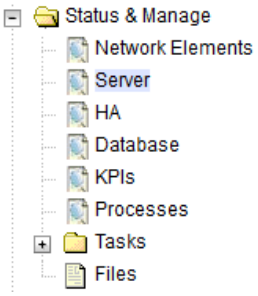
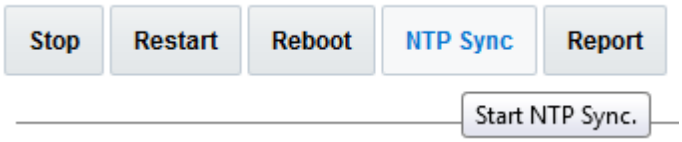
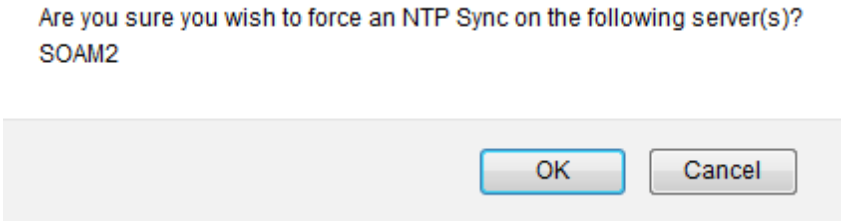
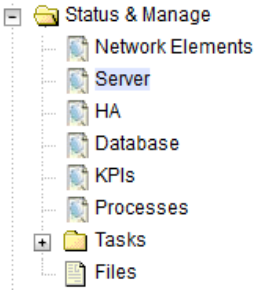
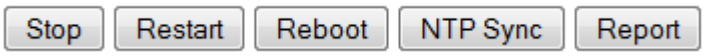
Step#	Procedure	Description
This procedure performs recovery if at least 1 DSR APIGW Database server is available Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	Workarounds	Refer to Appendix B Workarounds to understand/apply any workarounds required during this procedure.
2. ☐	Gather required materials	Gather the documents and required materials listed in Section Required Materials.

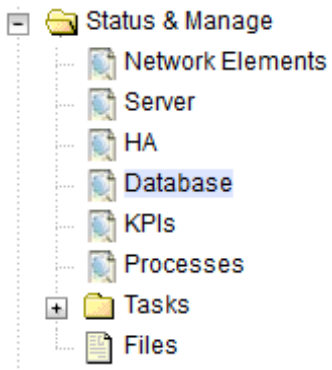
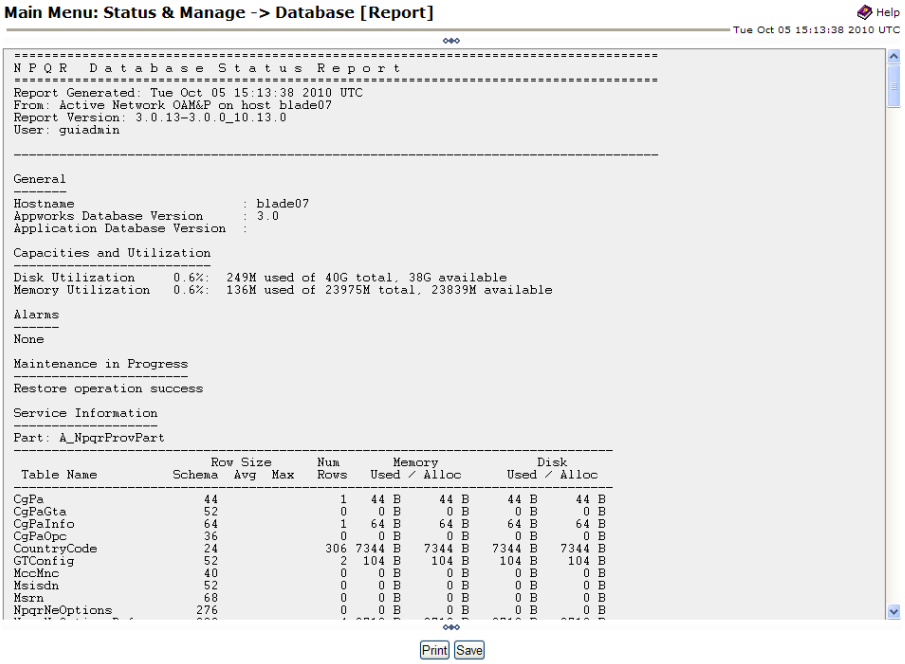
Step#	Procedure	Description
3. ☐	**DSR APIGW Database VIP GUI**: Login	1. Establish a GUI session on the DSR APIGW database server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
4. ☐	**Active DSR APIGW Database**: Set failed servers to OOS	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Set the **Max Allowed HA Role** to **OOS** for the failed servers. 4. Select **OK**.

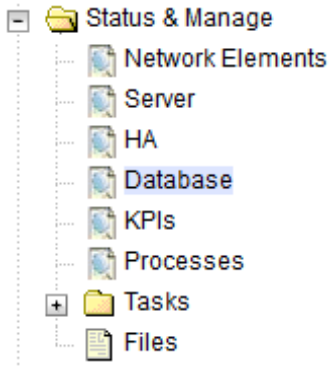
Step#	Procedure	Description
5. ☐	**Create VMs**: Recover the failed software	**For VMWare based deployments**: 1. For DSR APIGW database servers, execute the following procedures from reference [1]: a. Import DSR APIGW Database and Admin/Application OVAs (VMware). ***Note:*** If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Create DSR APIGW Database VMs (VMware). **For KVM/OpenStack based deployments**: 1. For DSR APIGW database servers, execute the following procedures from reference [1]: a. Import DSR APIGW Database and Admin/Application OVAs (OpenStack) ***Note:*** If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Create DSR APIGW Database VMs (OpenStack).
6. ☐	Repeat for remaining failed servers	If necessary, repeat step 5. for all remaining failed servers.

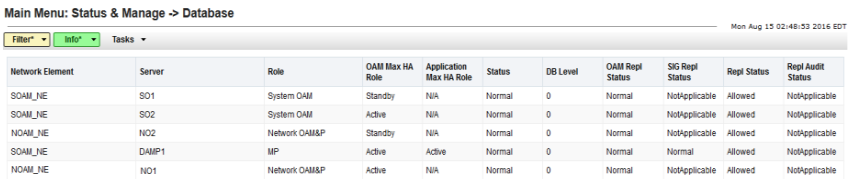
Step#	Procedure	Description
7. ☐	**DSR APIGW Database VIP GUI**: Login	1. Establish a GUI session on the DSR APIGW Database server by using the VIP IP address of the DSR APIGW Database server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. 
8. ☐	**DSR APIGW Database VIP GUI**: Recover standby DSR APIGW database	Install the second DSR APIGW database server by executing procedures from reference [1] Configure DSR APIGW Database.

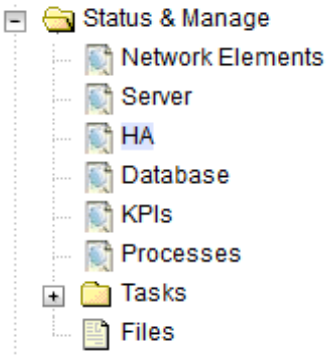
Step#	Procedure	Description
9. ☐	**DSR APIGW Database VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby DSR APIGW database server and click **Restart**. 
10. ☐	**DSR APIGW Database VIP GUI**: Set HA on standby DSR APIGW database	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the standby DSR APIGW database server and set it to **Active**. 4. Click **OK**.

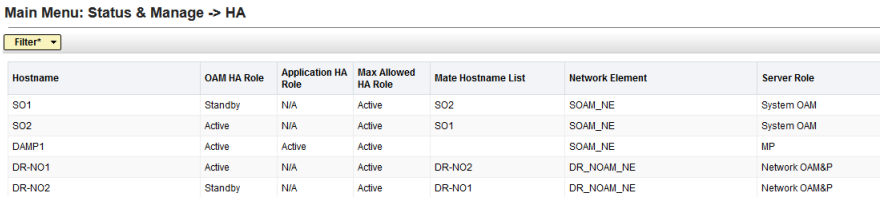
Step#	Procedure	Description
11. ☐	**Recovered Server**: Sync NTP	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **NTP Sync**.  3. Click **OK**. 
12. ☐	**DSR APIGW Database VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 
13. ☐	**Active DSR APIGW Database**: Perform key exchange between the active DSR APIGW database and recovered servers	1. Establish an SSH session to the active DSR APIGW database and login as **admusr**. 2. Execute this command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` ***Note:*** If an export server is configured, perform this step.

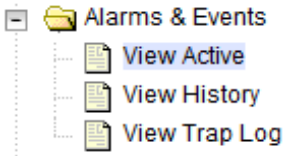
Step#	Procedure	Description
14. ☐	**DSR APIGW Database VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.  2. Select the active DSR APIGW database server and click **Report**. The following screen displays.  3. Click **Save** and save the report to your local machine.

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>15.
☐</td><td>Active DSR APIGW Database: Verify replication between servers</td><td>1. Log into the active DSR APIGW database using the SSH terminal as admusr user.
2. Execute this command:
<pre>$ sudo irepstat –m</pre>Output like below shall be generated:<pre>-- Policy 0 ActStb [DbReplication] ------------------------------
RDU06-MP1 -- Stby
  BC From RDU06-SO1 Active 0 0.50 ^0.17%cpu 42B/s A=none
  CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none
RDU06-MP2 -- Active
  BC From RDU06-SO1 Active 0 0.50 ^0.10%cpu 33B/s A=none
  CC To   RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none
RDU06-NO1 -- Active
  AB To   RDU06-SO1 Active 0 0.50 1%R 0.03%cpu 21B/s
RDU06-SO1 -- Active
  AB From RDU06-NO1 Active 0 0.50 ^0.04%cpu 24B/s
  BC To   RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s
  BC To   RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s</pre></td></tr>
<tr><td>16.
☐</td><td>DSR APIGW Database VIP GUI: Verify the database states</td><td>1. Navigate to Status and Manager > Database.
 

2. Verify the OAM Max HA Role is either Active or Standby for NOAM and the status is Normal.
 
</td></tr>
</table>

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>17.
☐</td><td>DSR APIGW Database VIP GUI: Verify the HA status</td><td>1. Navigate to Status and Manage > HA.
 

2. Select the row for all of the servers.
3. Verify the HA Role is either Active or Standby.
 

<table>
<tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th><th>Mate Hostname List</th><th>Network Element</th><th>Server Role</th></tr>
<tr><td>SO1</td><td>Standby</td><td>N/A</td><td>Active</td><td>SO2</td><td>SOAM_NE</td><td>System OAM</td></tr>
<tr><td>SO2</td><td>Active</td><td>N/A</td><td>Active</td><td>SO1</td><td>SOAM_NE</td><td>System OAM</td></tr>
<tr><td>DAMP1</td><td>Active</td><td>Active</td><td>Active</td><td></td><td>SOAM_NE</td><td>MP</td></tr>
<tr><td>DR-NO1</td><td>Active</td><td>N/A</td><td>Active</td><td>DR-NO2</td><td>DR_NOAM_NE</td><td>Network OAM&P</td></tr>
<tr><td>DR-NO2</td><td>Standby</td><td>N/A</td><td>Active</td><td>DR-NO1</td><td>DR_NOAM_NE</td><td>Network OAM&P</td></tr>
</table></td></tr>
<tr><td>18.
☐</td><td>DSR APIGW Database VIP GUI: Examine all alarms</td><td>1. Log into the DSR APIGW database VIP, if not already logged in.
2. Navigate to Alarms and Events > View Active.
 

3. Examine all active alarms and refer to the on-line help for how to address them.
4. If needed, contact My Oracle Support (MOS).</td></tr>
<tr><td>19.
☐</td><td>Back up and archive all the databases from the recovered system</td><td>Execute Appendix A DSR Database Backup to back up the configuration databases.</td></tr>
</table>

4. DSR APIGW Admin and Application Disaster Recovery Procedure

4.1 Recovery Scenario 1: Admin Server is Up and Running, and Application Server(s) is Lost

Procedure 3. Recovery Scenario 1: Admin Server is Up and Running, and Application Server(s) is Lost

Step #	Procedure	Description
This procedure recovers when an admin server is up and running and the application servers are lost. 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. ☐	**VMWare/ OpenStack**: Create lost application VMs	Create the application VMs, which have to be recovered, with same IP addresses. Refer to the following procedures from reference [1]: **For VMWare based deployments:** Create DSR APIGW Admin/Application VMs (VMWare). **For KVM/OpenStack based deployments:** Create DSR APIGW Admin/Application VMs (OpenStack).
2. ☐	**Admin Server**: Edit properties file	1. Log into the admin server. 2. Navigate to **/u02/app/oracle/scripts/**. `$ cd /u02/app/oracle/scripts/` 3. Edit the file **osgdr.properties**. Add respective property values to the file. 4. Feed in file with all the lost application server data. Refer to Appendix C for parameter details.
3. ☐	**Admin Server**: Execute application VM recovery script	1. Log into admin server. 2. Navigate to **/u02/app/oracle/scripts**. 3. Execute **recoverAppServers.py** to recover the application server.

4.2 Recovery Scenario 2: Application Servers are Up and Running, and Admin Server is Lost

Procedure 4. Recovery Scenario 2: Application Servers are Up and Running, and Admin Server is Lost

Step #	Procedure	Description
This procedure recovers when the application servers are up and running and the admin server is lost. 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. ☐	**OpenStack Controller**: Create lost admin server	Create the admin server with same IP addresses. Refer to the following procedures from reference [1]: **For VMWare based deployments:** Create DSR APIGW Admin/Application VMs (VMWare). **For KVM/OpenStack based deployments:** Create DSR APIGW Admin/Application VMs (OpenStack).
2. ☐	**OpenStack GUI**: Copy the .pem file (key-pair) used to create the VMs to the admin server in any location	1. Log into OpenStack controller console. 2. Copy the .**pem** file from the OpenStack controller to the admin server in any location. `$ scp -i /root/dsr-keypair.pem /root/ dsr-keypair.pem admusr@<aminserverip>:/u02` ***Note:*** PEM certificates are frequently used for web servers since they can easily be translated into readable data using a simple text editor. Generally, when a PEM encoded file is opened in a text editor, it contains very distinct headers and footers.
3. ☐	**Admin Server**: Edit properties file	1. Log into the admin server. 2. Navigate to **/u02/app/oracle/scripts/**. `$ cd /u02/app/oracle/scripts/` 3. Edit the file **osgdr.properties**. Add respective property values to the file. 4. Feed in file with all the lost admin server data and backup server details. Refer to Appendix C for parameter details.
4. ☐	**Admin Server**: Execute admin server recovery script	1. Log into admin server. 2. Navigate to **/u02/app/oracle/scripts**. 3. Execute **recoverAdminServer.py** to recover admin server.

4.3 Recovery Scenario 3: At Least One Application Server is Up, and Admin and Applications Servers are Lost

Procedure 5. Recovery Scenario 3: At Least One Application Server is Up, and Admin and Applications Servers are Lost

Step #	Procedure	Description
This procedure recovers when the admin server and the some of the application servers are lost. 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. ☐	**VMWare/ Openstack**: Create lost admin and application servers	Create the admin server and the lost application server with same IP addresses. Refer to the following procedures from reference [1]: **For VMWare based deployments:** Create DSR APIGW Admin/Application VMs (VMWare). **For KVM/OpenStack based deployments:** Create DSR APIGW Admin/Application VMs (OpenStack).
2. ☐	**OpenStack GUI**: Copy the .pem file (key-pair) used to create the VMs to the admin server in any location	1. Log into OpenStack controller console. 2. Copy the .**pem** file from the OpenStack controller to the admin server in any location. `$ scp -i /root/dsr-keypair.pem /root/ dsr-keypair.pem admusr@<aminserverip>:/u02` ***Note:*** PEM certificates are frequently used for web servers since they can easily be translated into readable data using a simple text editor. Generally, when a PEM encoded file is opened in a text editor, it contains very distinct headers and footers.
3. ☐	**Admin Server**: Edit properties file	1. Log into the admin server. 2. Navigate to **/u02/app/oracle/scripts/**. `$ cd /u02/app/oracle/scripts/` 3. Edit the file **osgdr.properties**. Add respective property values to the file. 4. Feed in file with all the lost admin server data and backup server details. Refer to Appendix C for parameter details.
4. ☐	**Admin Server**: Execute admin recovery script	1. Log into admin server. 2. Navigate to **/u02/app/oracle/scripts**. 3. Execute **recoverAdminServer.py** to recover admin server.
5. ☐	**Admin Server**: Execute application VM recovery script	1. Log into admin server. 2. Navigate to **/u02/app/oracle/scripts**. 3. Execute **recoverAppServers.py** to recover the application server.

4.4 Recovery Scenario 4: Admin and Application Servers are Lost

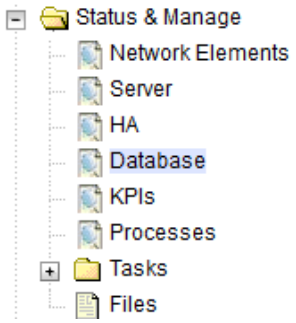
Procedure 6. Recovery Scenario 4: Admin and Application Servers are Lost

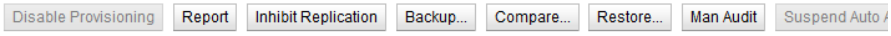
Step #	Procedure	Description
This procedure recovers the servers when the admin and the application servers are lost. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**OpenStack Controller**: Create lost admin server	Create the admin server with same IP addresses. Refer to the following procedures from reference [1]: **For VMWare based deployments:** Create DSR APIGW Admin/Application VMs (VMWare). **For KVM/OpenStack based deployments:** Create DSR APIGW Admin/Application VMs (OpenStack).
2. ☐	**OpenStack GUI**: Copy the .pem file (key-pair) used to create the VMs to the admin server in any location	1. Log into OpenStack controller console. 2. Copy the .**pem** file from the OpenStack controller to the admin server in any location. `$ scp -i /root/dsr-keypair.pem /root/ dsr-keypair.pem admusr@<aminserverip>:/u02` ***Note:*** PEM certificates are frequently used for web servers since they can easily be translated into readable data using a simple text editor. Generally, when a PEM encoded file is opened in a text editor, it contains very distinct headers and footers.
3. ☐	**Admin Server**: Edit properties file	1. Log into the admin server. 2. Navigate to **/u02/app/oracle/scripts/**. `$ cd /u02/app/oracle/scripts/` 3. Edit the file **osgdr.properties**. Add respective property values to the file. 4. Feed in file with all the lost admin server data and backup server details. Refer to Appendix C for parameter details.
4. ☐	**Admin Server**: Execute admin recovery script	1. Log into admin server. 2. Navigate to **/u02/app/oracle/scripts**. 3. Execute **recoverAdminServer.py** to recover admin server.
5. ☐	**Admin Server**: Execute application VM recovery script	1. Log into admin server. 2. Navigate to **/u02/app/oracle/scripts**. 3. Execute **recoverAppServers.py** to recover the application server.

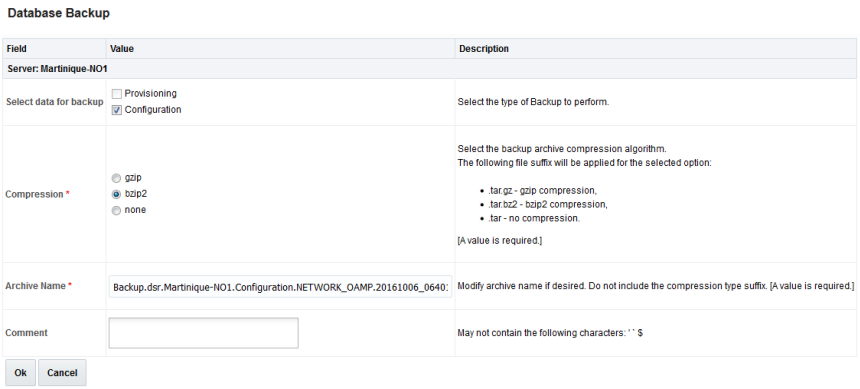
Appendix A. DSR Database Backup

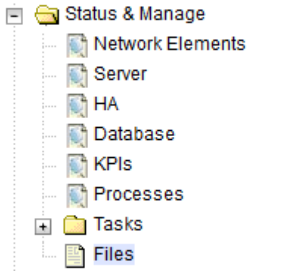
Procedure 7. Back Up the Provision and Configuration Data

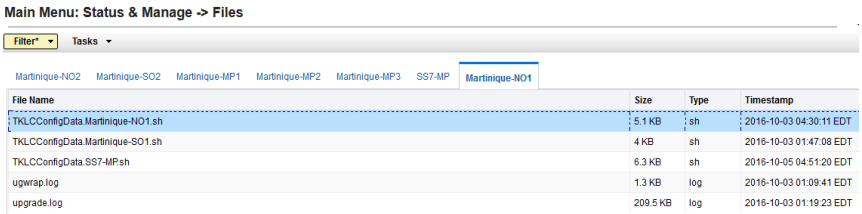
Step #	Procedure	Description
This procedure backs up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**NOAM/SOAM VIP**: Login	1. Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM/SOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

<table>
<tr><th>Step #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>2.
☐</td><td>NOAM/SOAM VIP: Back up configuration data for the system</td><td>1. Navigate to Status and Manage > Database.
 

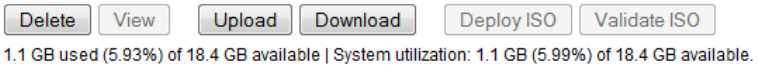
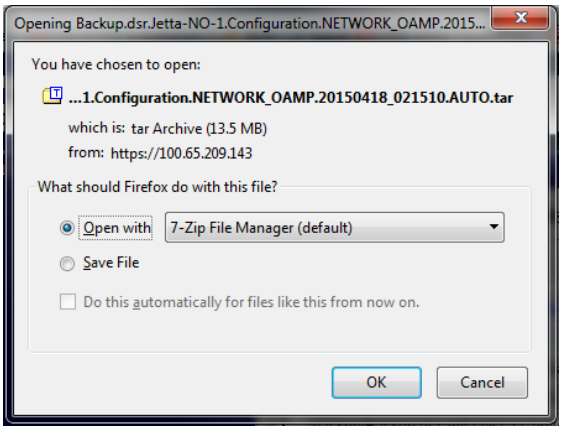
2. Select the active NOAM server and click Backup.
 

3. Make sure the Configuration checkbox is marked.
 

4. Enter a filename for the backup and click OK.</td></tr>
<tr><td>3.
☐</td><td>NOAM/SOAM VIP: Verify the backup file existence</td><td>1. Navigate to Status and Manage > Files.
 



2. Select the active NOAM or SOAM tab.
3. The files on this server display. Verify the existence of the backup file.</td></tr>
</table>

Step #	Procedure	Description
4. ☐	**NOAM/SOAM VIP**: Download the file to a local machine	1. From the previous step, choose the backup file. 2. Click **Download**.  3. Click **OK** to confirm the download. 
5. ☐	Upload the image to a secure location	Transfer the backed up image saved in the previous step to a secure location where the server backup files are fetched in case of a system disaster recovery.
6. ☐	Back up active SOAM	Repeat steps 2. through 5. to back up the active SOAM.

Appendix B. Workarounds

Procedure 8. Backup Directory

Step #	Procedure	Description
This procedure checks and creates a backup directory. 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/SOAM VIP Console: Determine if backup directory is created	1. Execute following command on console of Active NOAM/SOAM server (accessed via the VIP) and compare the output:
		`$ cd /var/TKLC/db/filemgmt/`
		`$ ls -ltr`
		2. Look for backup directory in the output.
		3. Check if directory is already created with correct permission.
		Directory will look like:
		`drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup`
		If the directory is already there with the correct permissions, then skip steps 2 and 3.
		4. If directory is not with right permissions then execute step 3; otherwise go to next step.

2.
☐
	NOAM/SOAM VIP Console: Create backup directory	1. Assuming the working directory is **/var/TKLC/db/filemgmt/**; otherwise, do
		`$ cd /var/TKLC/db/filemgmt/`
		2. Create the backup directory.
		`$ mkdir backup`

3.
☐
	NOAM/SOAM VIP Console: Change permissions of backup directory	1. Verify directory is created:
		`$ ls -ltr /var/TKLC/db/filemgmt/backup`
		A **No such file or directory** error should not display; instead an empty directory should show total 0 as content.
		2. Change permissions to the backup directory.
		`$ chmod 770 /var/TKLC/db/filemgmt/backup`
		3. Change ownership to the backup directory.
		`$ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup`
		The backup directory should look like:
		`drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15 backup`

Step #	Procedure	Description

4. □	**NOAM/SOAM VIP console:** Copy the backup file which we need to restore in backup directory	1. Copy the backup file to backup directory.
		`$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup`
		2. Verify the current working directory.
		`$ cd /var/TKLC/db/filemgmt/backup`
		3. Change permissions of files inside backup directory.
		`$chmod 666 Backup.*`
		4. Change ownership of files inside backup directory.
		`$ sudo chown -R awadmin:awadm Backup.*`

Appendix C. OCSG DR Properties File

Table 4: OCSG DR Properties File

Section	Parameter Name	Description
Admin	servers	IMI Interface address of Admin Server. servers = ["AdminServer: xxx.xxx.xxx.xxx "] Note: It is mandatory to follow the name of Admin server as 'AdminServer' This is the DSRAPIGW DB server address where data is backed up. DR procedure uses this data.
Admin	xmiInterface	XMI Interface address of Admin Server. xmiInterface = ["AdminServer: xxx.xxx.xxx.xxx "]
Admin	backupServer	Provide the IMI VIP of DSR API GW Database. Admin server should have access to this server using the key/pem file. This is the location in the DSRAPIGW DB server where the data should be backed up. For example, backupServer = xxx.xxx.xxx.xxx
Admin	backupDomain	Full path including the DSR API GW domain folder name to where the DSR API GW files need to be backed up on backup server. For example, backupDomain = /var/TKLC/db/filemgmt/backup/services-gatekeeper-domain
App	servers	Add application server name and IP. Add comma separated entries for multiple servers. For example, servers = ["AppServer1:xxx.xxx.xxx.xxx", "AppServer2:xxx.xxx.xxx.xxx"] Note: It is mandatory to follow the name of application servers as 'AppServer1', 'AppServer2' etc.

Section	Parameter Name	Description
App	xmiInterfaces	XMI Interface address for all AppServers in [“Ip1”,”Ip2”…] format. For example, xmiInterfaces = ["AppServer1: xxx.xxx.xxx.xxx ", "AppServer2: xxx.xxx.xxx.xxx "]
App	xsiInterfaces	XSI Interface address for all AppServers in [“Ip1”,”Ip2”…] format. For example, xsiInterfaces = ["AppServer1: xxx.xxx.xxx.xxx ", "AppServer2: xxx.xxx.xxx.xxx "] To add multiple XSIs to each AppServer the format should be, [“AppServer1:XSI1-IP”,”AppServer2:XSI2”,”AppServer2:XSI1-IP”,”AppServer2:XSI2”]
App	exteralLoadbalancerIP	IP used to publish T8 APIs. This IP is used when displaying T8 API access URLs in Partner and API management Portal. exteralLoadbalancerIP = xxx.xxx.xxx.xxx
Servers	cleanUpBeforeInstall	If the script failed to execute while running, the server is in a bad shape for a fresh install. Keeping cleanUpBeforeInstall as **yes** cleans up the server and makes it ready for script re-run.
Servers	ntp	Provide NTP server IP. ntp = xxx.xxx.xxx.xxx
Servers	mtu	Maximum transmission unit. The script copies multiple files from admin server to application server. Before copying the MTU has to be set. Recommended value is **9000**. mtu = 9000
Servers	apiroot	This variable is part of the API creation. <apiroot> is prefixed to the context uri of the APIs exposed. For example, the API name of Device triggering is **apiroot-dt**
Servers	dsrMpList	Provide DSR MP XSI Ip list in format, MP1-XSI-IP:port,MP2-XSI1-IP:port…..
Files	pemfile	Provide the .pem file location. pemfile = /u02/software/ocsg-db-key.pem
Files	logfile	Custom log file for installation. Change log file name, if required. logfile = ocsg_install.log
Files	presentFolder	The scripts are in this location. This property should not be changed presentFolder = /u02
Files	targetFolder	The scripts are copied to this location. This v should not be changed targetFolder = /u03

Section	Parameter Name	Description
Files	targetPath	Provide the location of the scripts. This property should not be changed. targetPath = /app/oracle/
Files	scripts	Provide the folder name where scripts need to be stored. This property should not be changed. scripts = scripts
Files	extendWizard	Custom scripts are present here. This property should not be changed. extendWizard = extend_wizard/
Files	SCEFPackage_EAR	Default EAR file name. This property should not be changed. SCEFPackage_EAR = SCEFHandlers.ear
Files	nodemgr	Node manager service file name. This property should not be changed. Nodemgr = nodemgr
Files	DefaultJar	Location of ocsg_generic_jar. This property should not be changed. defaultJar = /usr/TKLC/dsrapigw/ocsg_generic_jar
Files	volumeName	Provide the Volume name. This property should not be changed. volumeName = ocsgv
Files	volumeSize	Volume size in GB. Script creates a new volume of this size. This field should not be changed. volumeSize = 10
Files	inventoryLoc	Inventory log location of OCSG. This property should not be changed. inventoryLoc = /u02/inventory
Credentials	mysqlJdbcServerUrl	MySQL DB credentials. Provide IMI VIP of the DSR API GW database setup. jdbc:mysql://<db-server-ip>:15616/gatekeeper For example, mysqlJdbcServerUrl = jdbc:mysql://30.30.30.17:15616/gatekeeper
Credentials	mysqlUserName	This property should not be changed. mysqlUserName = awadmin ***Note:*** MySQL password is the default comcol password. It is in the dsrapigw_default_params.rsp file.
Credentials	weblogicUser	Provide the DSR API GW Admin portal credentials. weblogicUser = weblogic weblogicPassword = tekelec123
Credentials	weblogicPassword	
Credentials	nodeManagerUser	Provide the Nodemanager credentials to use in all Admin and

Section	Parameter Name	Description
Credentials	nodeManagerPassword	AppServers. nodeManagerUser = nodemanager nodeManagerPassword = tekelec123
Credentials	operatorUser	A new operator is created with thes details to access partner relationship management portal. operatorUser = oracleop3 operatorPassword = tekelec123
Credentials	operatorPassword	
Credentials	adminServerUser	The ssh user name in Admin and AppServers. adminServerUser = admusr appServerUser = admusr
Credentials	appServerUser	
Ports	adminListenPort appListenPort appListenPortSSL	These are the default ports opened on IMI network and should not be changed. These ports are used only for internal communication. adminListenPort = 7001 appListenPort = 8001 appListenPortSSL = 8002
Ports	adminIMIPorts adminXMIPorts	Ports to enable on the IP firewall of the Admin server. adminIMIPorts = 7001,5556,7002,9876,8050,3075,9090,7 adminXMIPorts = 9002
Ports	appIMIPorts appXMIPorts appXSIPorts	Ports to enabled on the IP firewall of the AppServers. appIMIPorts = 8001,8002,9876,5556,8050,3075,9090,7 9002 appXSIPorts = 10001,10002

Appendix D. 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 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, and 365 days a year.

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.

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 display 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 displays. 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.