Oracle® Communications

Diameter Signaling Router

DSR APIGW Disaster Recovery Guide

Release 8.4

F12355-01

April 2019

ORACLE®

Oracle Communications Diameter Signaling Router, DSR APIGW Disaster Recovery Guide

CAUTION: Use only the DR procedures included in the Disaster Recovery Kit.

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

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 MOS in the Appendix section.

Table of Contents

List of Procedures

List of Tables

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: Please note that 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

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
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
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

Table 2: Terminology

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 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 is up and running, App server(s) lost*]	• All Application servers failed
Recovery of Admin server [*Recovery Scenario 2: App servers are up and running, Admin server lost*]	• Admin server failed
Recovery of Admin and lost Application servers [*Recovery Scenario 3: At least one App server is up, Admin and App server(s) lost*]	• Admin server failed • One App server intact
Recover of both Admin and Application servers *[Recovery Scenario 4: Admin and App servers lost*]	• Both Admin and App 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:

1. A hardcopy of this document (E76332) and hardcopies of all documents in the reference list
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer's site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR APIGW recent backup files: electronic backup file (preferred) or hardcopy of all DSR APIGW configuration and provisioning data.
4. Latest Network Interface data; XSI interface lost
5. The ocsgdr.praperties file to fill-in the parameter details
6. **recoverAdminServer.py** script to recover Admin server
7. ***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 below 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 is up and running, App server(s) lost	Section Recovery Scenario 1: Admin is up and running, App server(s) lost
4	• App servers are up and running, Admin server lost	Section Recovery Scenario 2: App servers are up and running, Admin server lost
5	• At least one App server is up, Admin and App server(s) lost	Section Recovery Scenario 3: At least one App server is up, Admin and App server(s) lost
6	• Admin and App servers lost	Section Recovery Scenario 4: Admin and App servers lost

3. DSR APIGW Database Disaster Recovery Procedure

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

Before disaster recovery, users must properly evaluate the outage scenario. This check ensures that 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 below Recovery Scenarios, the backup directory may not be there in the system as system will be DRed.

In this case, please refer to Workarounds for Issues not fixed in this Release, this will provide steps to check and create the backup directory.

File format for recovery will be when back was taken. Generally back file is in format below.
For example:-
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 will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual detailed steps are in Procedure 1. 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.

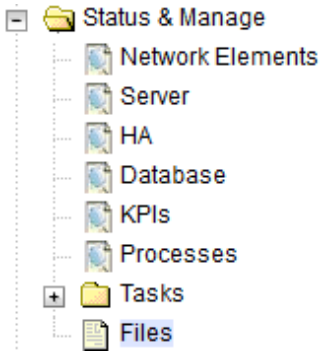
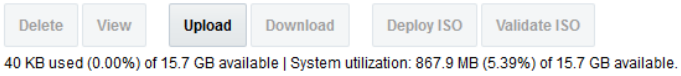
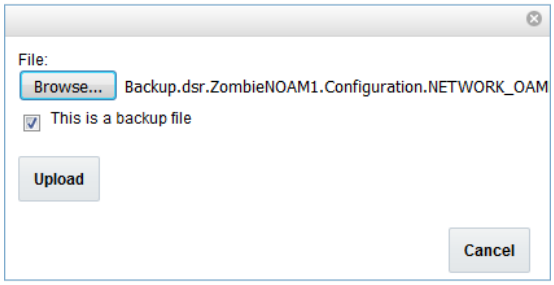
- Reconfigure the DSR Application

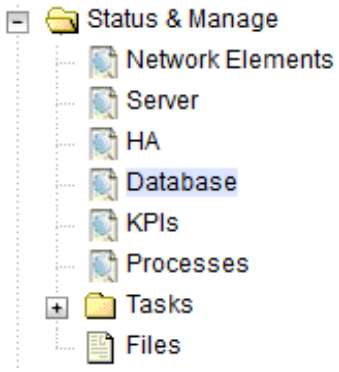
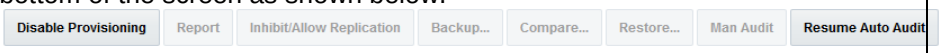
Restart process and re-enable provisioning replication

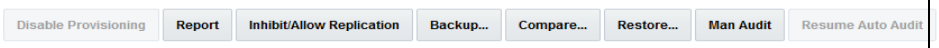
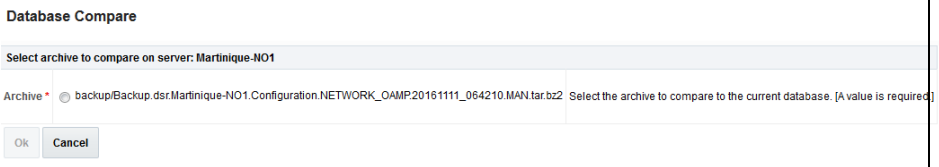
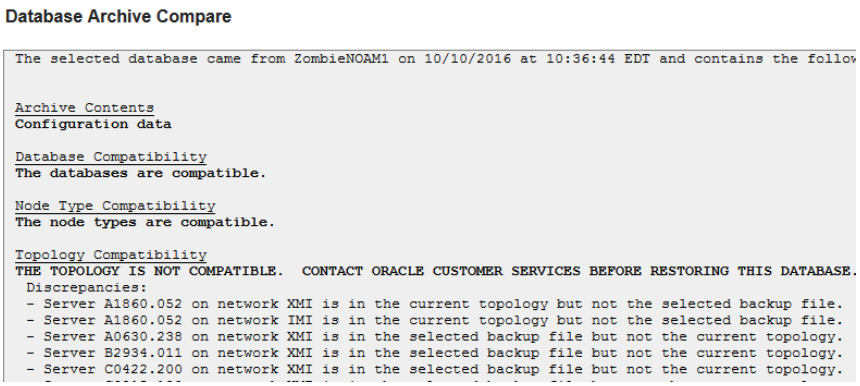
Procedure 1. Recovery Scenario 1

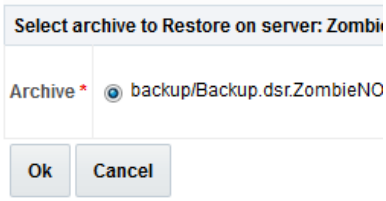
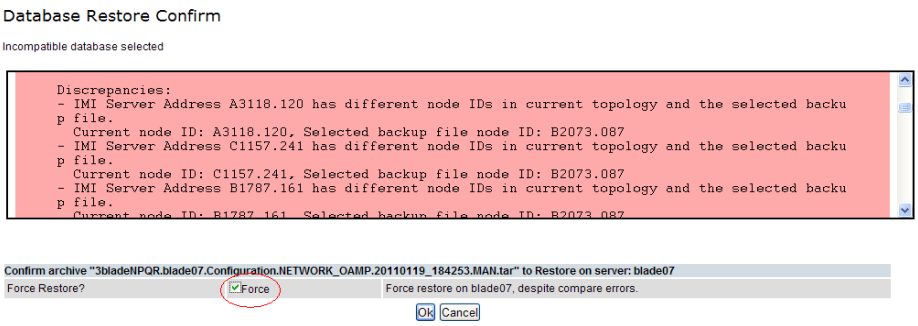
Step#	Procedure	Description
This procedure performs recovery if both DSR APIGW database servers are failed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Workarounds**	Refer to **Workarounds for Issues not fixed in this Release** 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 of importing OVA] b. Create DSR APIGW Database VMs (VMware) For KVM / Openstack based deployments: 2. 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 of importing OVA] b. Create DSR APIGW Database VMs (Openstack)
4. ☐	**Obtain Latest Database Backup and Network Configuration Data.**	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. From required materials list in **Section** Required Materials; use site survey documents and Network Element report (if available), to determine network configuration data.

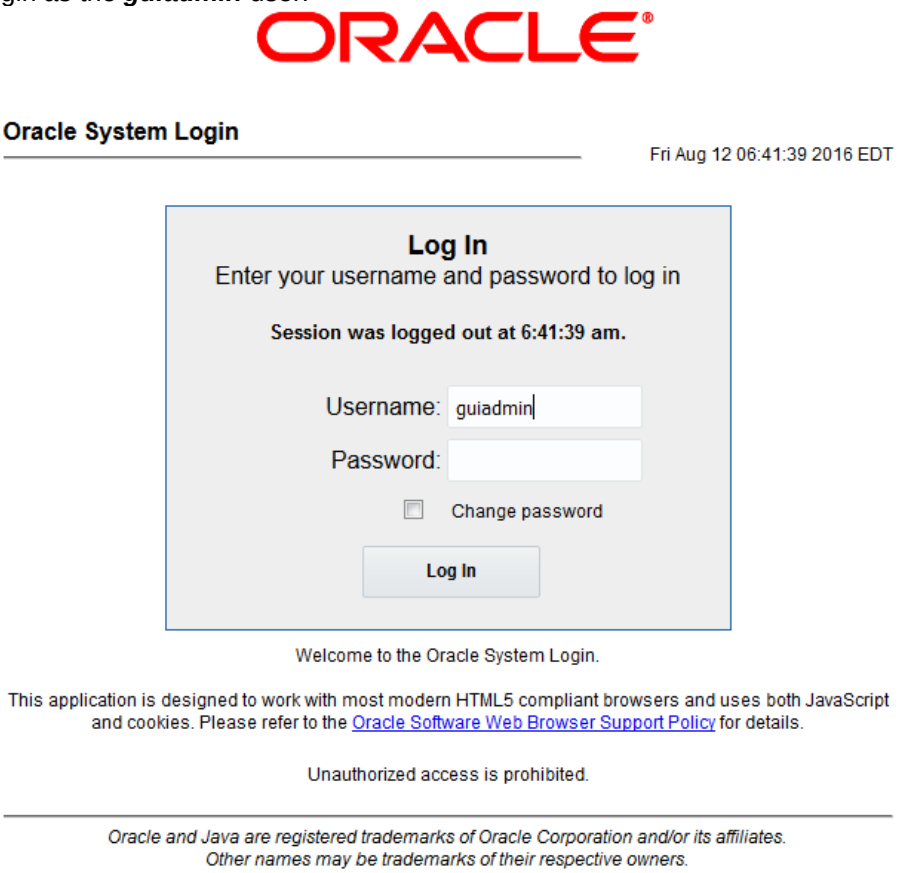
Step#	Procedure	Description
5. ☐	**Execute DSR APIGW Installation Procedure for the Database (DB1) server**	Verify the networking data for Network Elements **Note:** Use the backup copy of network configuration data and site surveys (Step 2) **Execute** installation procedures for the **Database (DB1) server** from reference [1]: **Configure DSR APIGW Database**
6. ☐	**DSR APIGW Database GUI:** Login	Login to the Database (DB1) GUI as the ***guiadmin*** user: 

Step#	Procedure	Description
7. ☐	**DSR APIGW Database GUI:** Upload the Backed up Database File	Browse to **Main Menu->Status & Manage->Files**  Select the Active **DSR APIGW Database (DB1)** server. Click on **Upload** as shown below and select the file *"NO Provisioning and Configuration:"* file backed up after initial installation and provisioning.  1. Click on **Browse** and locate the backup file 2. Check **This is a backup file** Box 3. Click on Open as shown below.  Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

Step#	Procedure	Description
8. ☐	**DSR APIGW Database GUI:** Disable Provisioning	Click on **Main Menu->Status & Manage->Database**  Disable Provisioning by clicking on **Disable Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to disable Provisioning.  The message *"Warning Code 002"* will appear.

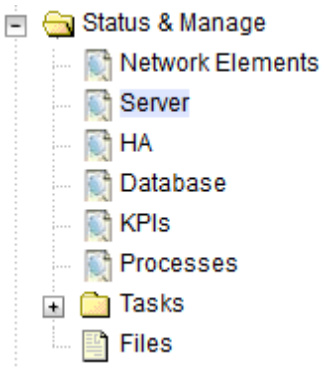
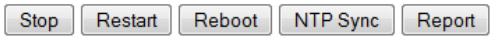
Step#	Procedure	Description
9. ☐	**DSR APIGW Database GUI:** Verify the Archive Contents and Database Compatibility	Select the **Active DSR APIGW Database** server and click on the **Compare**.  The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix D: My Oracle Support (MOS).  **Note:** Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one **DSR APIGW Database**: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

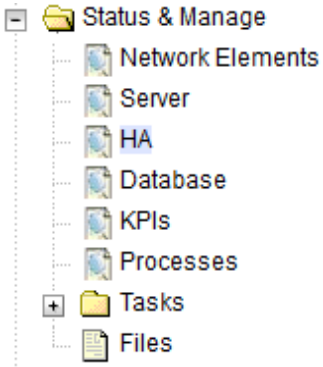
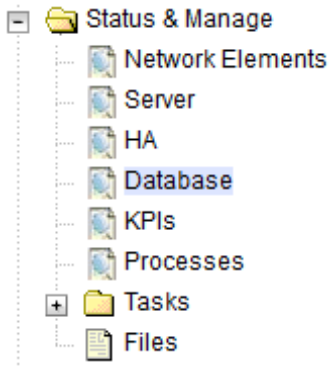
Step#	Procedure	Description
10. ☐	**ACTIVE DSR APIGW Database:** Restore the Database	Click on **Main Menu->Status & Manage->Database** Select the **Active DSR APIGW Database** server, and click on **Restore** as shown below. The following screen will be displayed. Select the proper back up provisioning and configuration file.  Click **OK** Button. The following confirmation screen will be displayed. **Note:** You will get a database mismatch regarding the NodeIDs of the servers. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix D: My Oracle Support (MOS). Select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.  **Note:** After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.

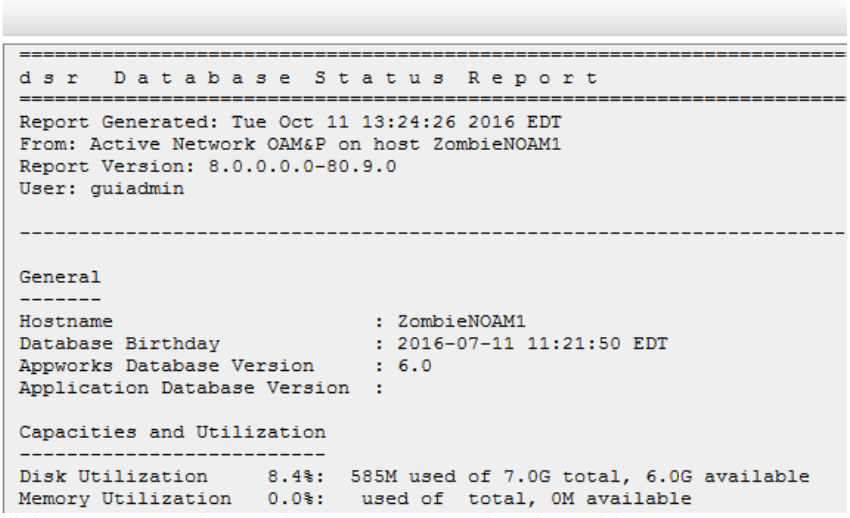
Step#	Procedure	Description
11. ☐	**DSR APIGW Database VIP GUI:** Login	Establish a GUI session on the DSR APIGW Database server by using the VIP IP address of the DSR APIGW Database server. Open the web browser and enter a URL of: `http://<Primary_DSR APIGW Database_VIP_IP_Address>` Login as the ***guiadmin*** 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 will indicate that the backup is complete and the system is stabilized. 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) **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.

Step#	Procedure	Description
13. ☐	**DSR APIGW Database NOAM:** Login	Login to the recovered Active DSR APIGW Database via SSH terminal as ***admusr*** user.
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**

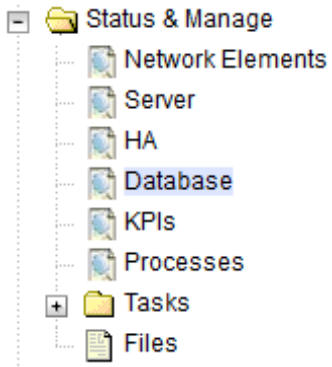
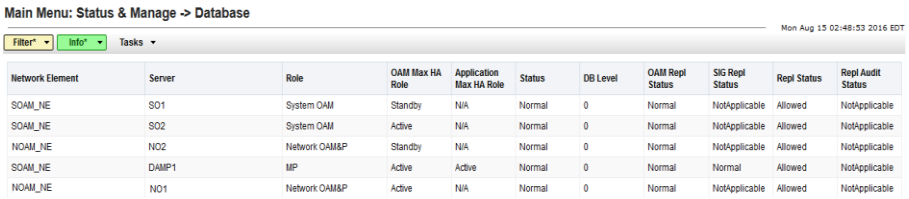
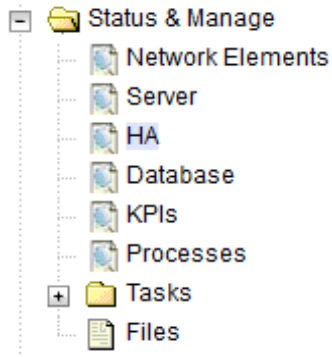
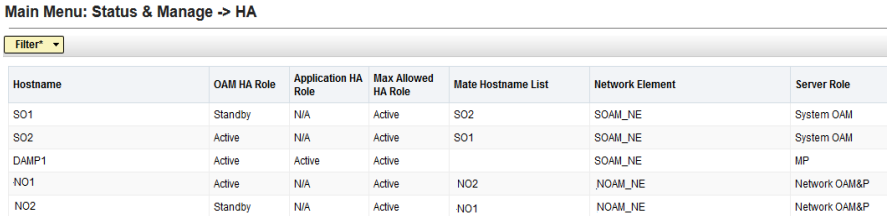
15. ☐	**Active DSR APIGW Database (DB1):** Correct the RecognizedAuthority table	Establish an SSH session to the active **DSR APIGW Database**, login as ***admusr***.
		
		Execute the following command:
		`$ sudo top.setPrimary`
		`- Using my cluster: A1789`
		`- New Primary Timestamp: 11/09/15 20:21:43.418`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

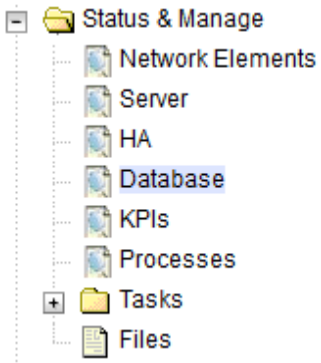
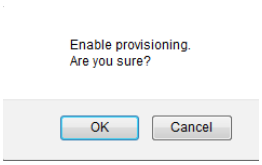
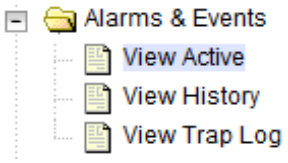
16. ☐	**DSR APIGW Database VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby DSR APIGW Database server and click on **Restart**. 

Step#	Procedure	Description
17. ☐	**DSR APIGW Database VIP GUI:** Set HA on Standby DSR APIGW Database	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the standby DSR APIGW Database server, set it to **Active** Press **OK**
18. ☐	**DSR APIGW Database VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**  Select the **active** DSR APIGW Database server and click on the **Report** button at the bottom of the page. The following screen is displayed:

Step#	Procedure	Description
		Main Menu: Status & Manage -> Database [Report]  Click on **Save** and save the report to your local machine.

19.
☐
	ACTIVE DSR APIGW Database: Verify Replication Between Servers.	Login to the Active DSR APIGW Database via SSH terminal as ***admusr*** user.
		Execute the following command:
		$ sudo irepstat –m
		
		Output like below shall be generated:
		`-- 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`

Step#	Procedure	Description
20. ☐	**DSR APIGW Database VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for DSR APIGW Database and that the status is “Normal” as shown below: 
21. ☐	**DSR APIGW Database VIP GUI:** Verify the HA Status	Click on **Main Menu->Status and Manage->HA**  Select the row for all of the servers Verify that the “HA Role” is either “Active” or “Standby”. 

Step#	Procedure	Description
22. ☐	**DSR APIGW Database GUI:** Enable Provisioning	Click on **Main Menu->Status & Manage->Database**  Enable Provisioning by clicking on **Enable Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to enable Provisioning. 
23. ☐	**DSR APIGW Database VIP GUI:** Examine All Alarms	Login to the DSR APIGW Database VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact Appendix D: My Oracle Support (MOS)
24. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute DSR Database Backup.

3.1.2 Recovery Scenario 2: Partial Server Outage with one Database server intact

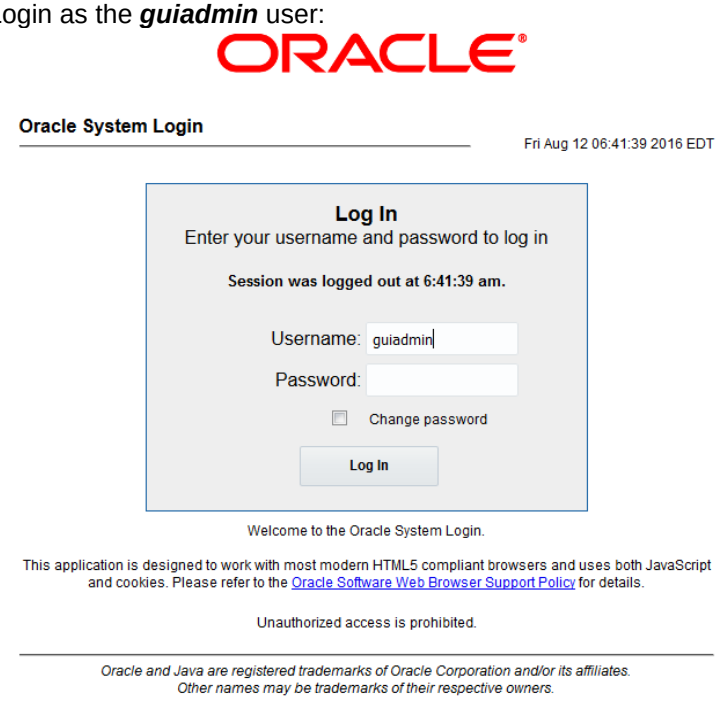
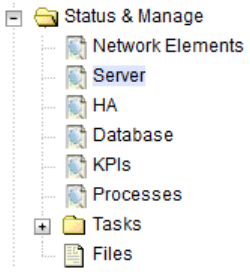
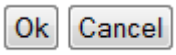
For a partial server outage with a DSR APIGW Database server intact and available. All other servers are recovered using recovery procedures for software. Database replication from the active NOAM server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The major activities are summarized as follows:

Recover **Standby DSR APIGW Database** server *(if needed)* by recovering software and the database.

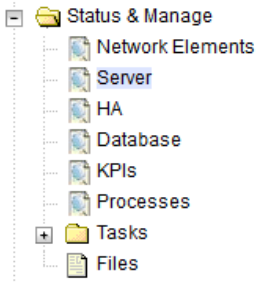
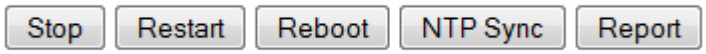
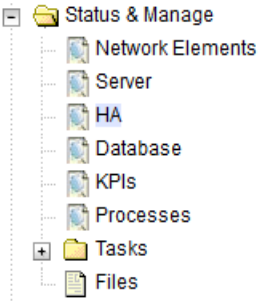
- Recover the software.

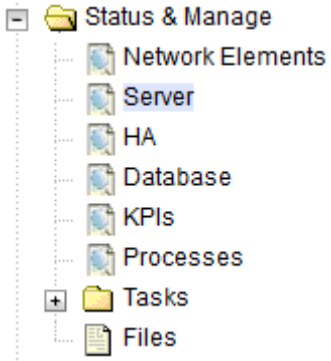
Procedure 2. Recovery Scenario 2

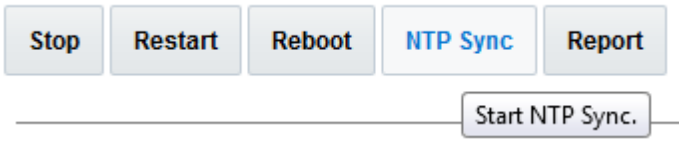
Step#	Procedure	Description
This procedure performs recovery if at least 1 DSR APIGW Database server is available Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Workarounds**	Refer to **Workarounds for** Issues not fixed in this Release to understand any workarounds required during this procedure.
2. ☐	**Gather Required Materials**	Gather the documents and required materials listed in **Section Required** Materials

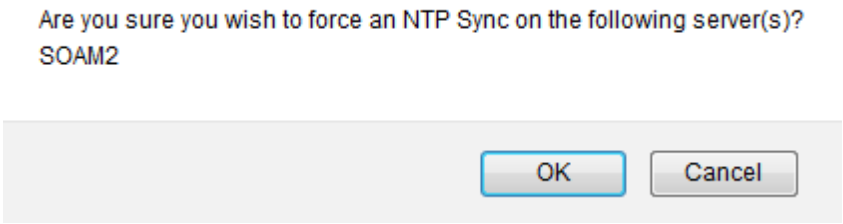
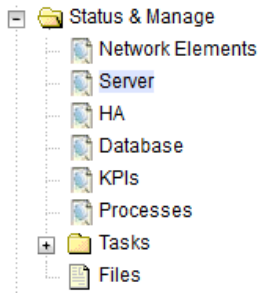
Step#	Procedure	Description
3. ☐	**DSR APIGW Database VIP GUI:** Login	Establish a GUI session on the DSR APIGW Database server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
4. ☐	**Active DSR APIGW Database:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit** Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. Select **Ok** 

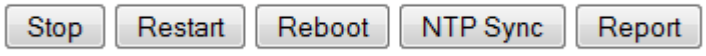
Step#	Procedure	Description
5. ☐	**Create VMs Recover the Failed Software**	For VMWare based deployments: 1. For DSR APIGW Database execute the following procedures from reference [1]: a. Import DSR APIGW Database and Admin/Application OVAs (VMware) [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Create DSR APIGW Database VMs (VMware) For KVM / Openstack based deployments: 3. 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 of importing OVA] b. Create DSR APIGW Database VMs (Openstack)
6. ☐	**Repeat for Remaining Failed Servers**	If necessary, repeat **step 5** for all remaining failed servers.
7. ☐	**DSR APIGW Database VIP GUI:** Login	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>` Login as the ***guiadmin*** user: 

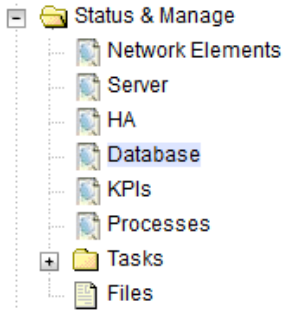
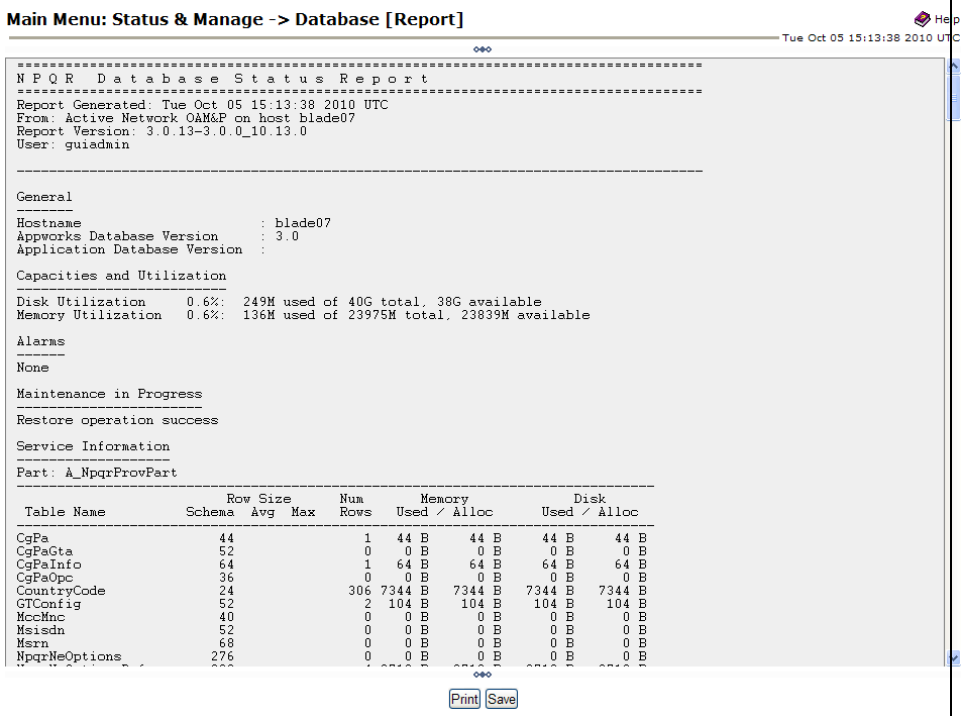
Step#	Procedure	Description
8. ☐	**DSR APIGW Database VIP GUI:** Recover Standby DSR APIGW Database	Install the second DSR APIGW Database server by executing procedures from reference [1], **Configure DSR APIGW Database** **Note:** If Topology or nodeId alarms are persistent after the database restore, refer to Workarounds for Issues not fixed in this Release or the next step below.
9. ☐	**DSR APIGW Database VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby DSR APIGW Database server and click on **Restart**. 
10. ☐	**DSR APIGW Database VIP GUI:** Set HA on Standby DSR APIGW Database	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the standby DSR APIGW Database server, set it to **Active** Press **OK**

<table>
<tr><th>Step#</th><th>Procedure</th><th>Description</th></tr>
<tr><td>11.
☐</td><td>Recovered Server: Sync NTP</td><td>Navigate to Status & Manage -> Server
 

Select the Recovered server and click NTP Sync button
 

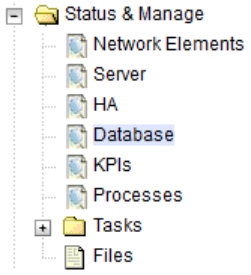
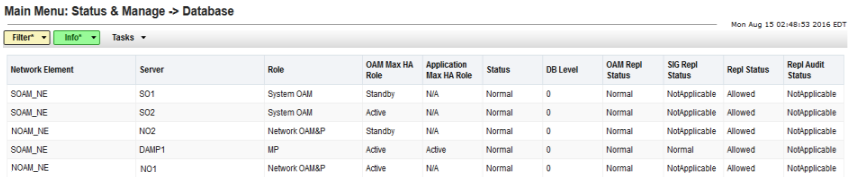
Click Ok
 
</td></tr>
<tr><td>12.
☐</td><td>DSR APIGW Database VIP GUI: Restart DSR application</td><td>Navigate to Main Menu->Status & Manage->Server,
 

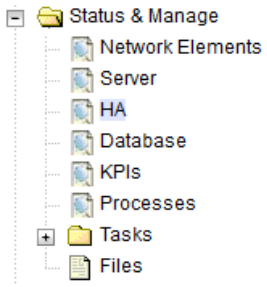
Select the recovered server and click on Restart.
 
</td></tr>
</table>

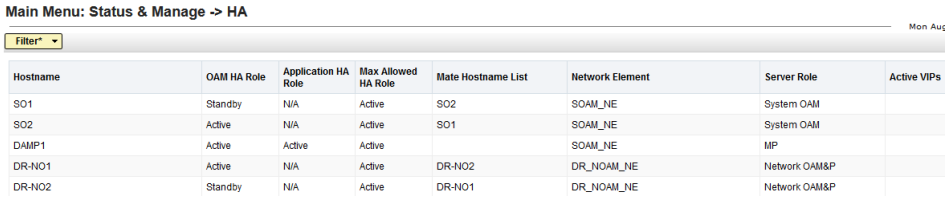
Step#	Procedure	Description
13. ☐	**ACTIVE DSR APIGW Database:** Perform key exchange between the active- DSR APIGW Database and recovered servers.	Establish an SSH session to the Active DSR APIGW Database, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **Note:** If an export server is configured, perform this step.
14. ☐	**DSR APIGW Database VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**  Select the **active** DSR APIGW Database server and click on the **Report** button at the bottom of the page. The following screen is displayed:  Click on **Save** and save the report to your local machine.

Step#	Procedure	Description

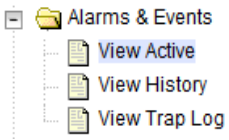
15. ☐	**ACTIVE DSR APIGW Database:** Verify Replication Between Servers.	Login to the Active DSR APIGW Database via SSH terminal as ***admusr*** user. Execute the following command:
		`$ sudo irepstat –m`
		Output like below shall be generated:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- 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`

16. ☐	**DSR APIGW Database VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and that the status is “Normal” as shown below: 

<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>Click on Main Menu->Status and Manage->HA
 

Select the row for all of the servers
Verify that 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><th>Active VIPs</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><td></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><td></td></tr>
<tr><td>DAMP1</td><td>Active</td><td>Active</td><td>Active</td><td></td><td>SOAM_NE</td><td>MP</td><td></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><td></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><td></td></tr>
</table></td></tr>
<tr><td>18.
☐</td><td>DSR APIGW Database VIP GUI: Examine All Alarms</td><td>Login to the DSR APIGW Database VIP if not already logged in.

Navigate to Main Menu->Alarms & Events->View Active
 

Examine all active alarms and refer to the on-line help on how to address them.

If needed contact Appendix D: My Oracle Support (MOS).</td></tr>
<tr><td>19.
☐</td><td>Backup and Archive All the Databases from the Recovered System</td><td>Appendix A DSR Database Backup for back up the Configuration databases:</td></tr>
</table>

4. DSR APIGW Admin and Application Disaster Recovery Procedure

4.1 Recovery Scenario 1: Admin is up and running, App server(s) lost

Procedure 3. Recovery Scenario 1: Admin is up and running, App server(s) lost

Step #	Procedure	Description
The intent of this procedure is to recover when Admin 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 App VMs	Create the Application VMs, which has to be recovered, with same IP addresses. Refer to the following procedures from reference [1]: For VMWare based deployments: 1. Create DSR APIGW Admin/Application VMs (VMWare) For KVM/Openstack based deployments: 1. Create DSR APIGW Admin/Application VMs (Openstack)
2. ☐	**Admin Server:** Edit properties file	1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts/*** `$ cd /u02/app/oracle/scripts/` 3. Edit the file **osgdr.properties**. Add respective property values in the file. Feed in file with all the lost App servers data. Refer to Appendix C for parameter details.
3. ☐	**Admin Server:** Execute App VM recovery script	From Admin server, execute the script as follows: 1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts*** 3. Execute ***recoverAppServers.py*** to recover Application server.

4.2 Recovery Scenario 2: App servers are up and running, Admin server lost

Procedure 4. Recovery Scenario 2: App servers are up and running, Admin server lost

Step #	Procedure	Description
The intent of this procedure is to recover when 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: 1. Create DSR APIGW Admin/Application VMs (VMWare) For KVM/Openstack based deployments: 1. Create DSR APIGW Admin/Application VMs (Openstack)
2. ☐	**Openstack GUI:** Copy the .pem file (key-pair) used to create the VMs to Admin server in any location.	1. Login to Openstack controller console 2. Copy the pem file from the opentack 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 as 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. Refer to **Error! Reference source not found.** for creating a PEM file.
3. ☐	**Admin Server:** Edit properties file	1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts/*** `$ cd /u02/app/oracle/scripts/` 3. Edit the file **osgdr.properties**. Add respective property values in the file. Feed in **osgdr.properties** file with the lost Admin server data and back up server details. Refer to Appendix C for parameter details.
4. ☐	**Admin Server:** Execute Admin server recovery script	From Admin server, execute the script as follows: 1. Login to **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 App server is up, Admin and App server(s) lost

Procedure 5. Recovery Scenario 3: At least one App server is up, Admin and App server(s) lost

Step #	Procedure	Description
The intent of this procedure is to recover when Admin 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 server	Create the Admin server and the lost App server with same IP addresses. Refer to the following procedures from reference [1]: For VMWare based deployments: 1. Create DSR APIGW Admin/Application VMs (VMWare) For KVM/Openstack based deployments: 1. Create DSR APIGW Admin/Application VMs (Openstack)
2.	**Openstack GUI:** Copy the .pem file (key-pair) used to create the VMs to Admin server in any location.	1. Login to Openstack controller console 2. Copy the pem file from the opentack 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 as 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. Refer to **Error! Reference source not found.** for creating a PEM file.
3. ☐	**Admin Server:** Edit properties file	1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts/*** `$ cd /u02/app/oracle/scripts/` 3. Edit the file **osgdr.properties**. Add respective property values in the file. Feed in **osgdr.properties** file with the lost Admin server data and back up server details. Refer to Appendix C for parameter details.
4. ☐	**Admin Server:** Execute Admin server recovery script	From Admin server, execute the script as follows: 1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts*** 3. Execute ***recoverAdminServer.py*** to recover Admin server.

Step #	Procedure	Description
5. ☐	**Admin Server:** Execute App VMs recovery script	From Admin server, execute the script as follows: 1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts*** 3. Execute ***recoverAppServers.py*** to recover Application server.

4.4 Recovery Scenario 4: Admin and App servers lost

Procedure 6. Recovery Scenario 4: Admin and App servers lost

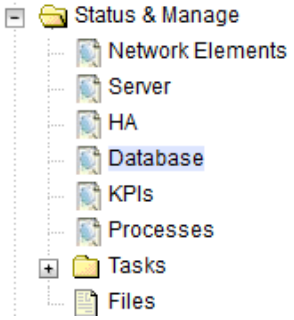
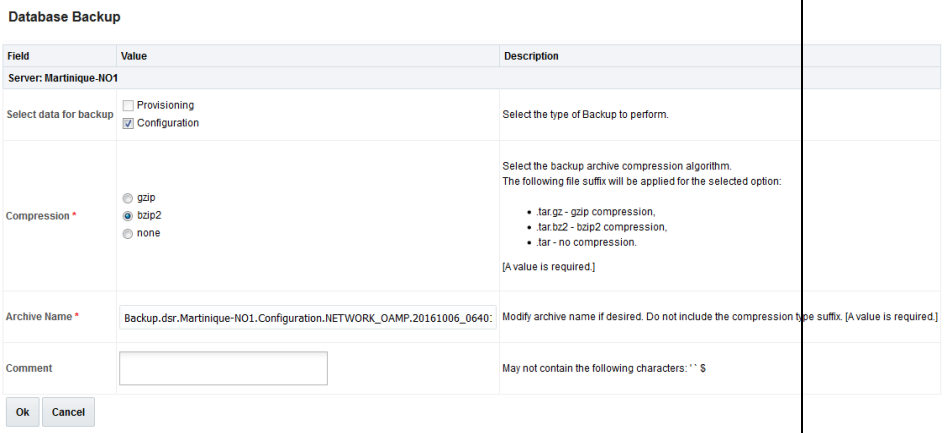
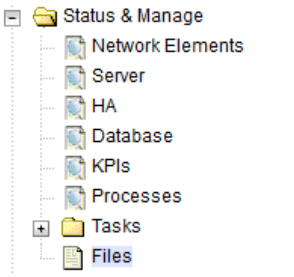
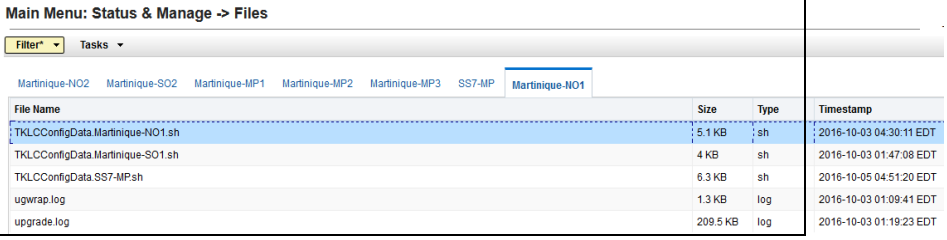
Step #	Procedure	Description
The intent of this procedure is to recover when Admin and the application servers are lost. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**VMWare/Openstack**: Create lost Admin server	Create the Admin server with same IP addresses. Refer to the following procedures from reference [1]: For VMWare based deployments: 2. Create DSR APIGW Admin/Application VMs (VMWare) For KVM/Openstack based deployments: 2. Create DSR APIGW Admin/Application VMs (Openstack)
2.	**Openstack GUI:** Copy the .pem file (key-pair) used to create the VMs to Admin server in any location.	1. Login to Openstack controller console 2. Copy the pem file from the opentack 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 as 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. Refer to **Error! Reference source not found.** for creating a PEM file.
3. ☐	**Admin Server:** Edit properties file	1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts/*** `$ cd /u02/app/oracle/scripts/` 3. Edit the file **osgdr.properties**. Add respective property values in the file. Feed in **osgdr.properties** file with the lost Admin server data and back up server details. Refer to Appendix C for parameter details.

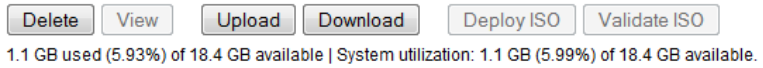
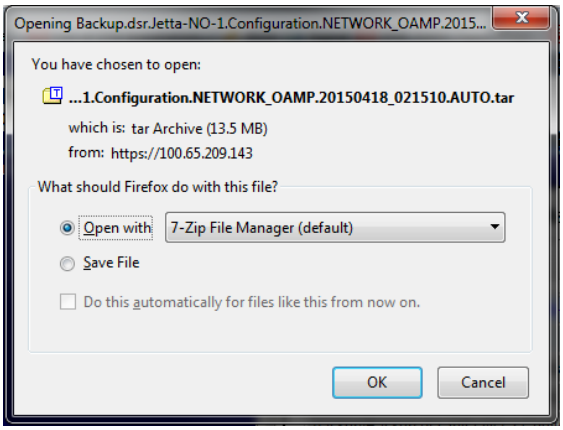
Step #	Procedure	Description
4. ☐	**Admin Server:** Execute Admin server recovery script	From Admin server, execute the script as follows: 1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts*** 3. Execute ***recoverAdminServer.py*** to recover Admin server.
5. ☐	**Admin Server:** Execute App VMs recovery script	From Admin server, execute the script as follows: 1. Login to **Admin** server 2. Navigate to ***/u02/app/oracle/scripts*** 3. Execute ***recoverAppServers.py*** to recover Application server.

Appendix A. DSR Database Backup

Procedure 7. Back up the provision and configuration data

STEP#	Procedure	Description
The intent of this procedure is to back 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	Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM/SOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

2. ☐	**NOAM/SOAM VIP:** Backup Configuration Data for the System	Navigate to **Main Menu -> Status & Manage -> Database**  Select the Active NOAM Server and Click on **Backup** button  Make sure that the checkboxes next to “Configuration” is checked.  Enter a filename for the backup and press **OK**
3. ☐	**NOAM/SOAM VIP:** Verify the backup file existence.	Navigate to **Main Menu -> Status & Manage -> Files**  

		Select the Active NOAM or SOAM tab. The files on this server will be displayed. Verify the existence of the backup file.
4. ☐	**NOAM/SOAM VIP:** Download the file to a local machine.	From the previous step, choose the backup file. Select the **Download** button  Select **OK** to confirm the download. 
5. ☐	**Upload the Image to 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 system disaster recovery.
6. ☐	**Backup Active SOAM**	Repeat **Steps 2 through 5** to back up the Active SOAM

Appendix B. Workarounds for Issues not fixed in this Release

Procedure 8. Backup directory

STEP#	Procedure	Description
This procedure will provide the steps to check and create 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	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`
		
		Look for backup directory in the output.
		Check if directory is already created with correct permission.
		Directory will look like:-
		
		drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup
		
		In case, directory is already there with right permissions then skip steps 2 and 3.
		If directory is not with right permissions then execute step 3.
		Otherwise go to next step.

2.
☐
	NOAM/SOAM VIP console: Create backup directory	Assuming present working directory is `/var/TKLC/db/filemgmt/`
		Otherwise, do
		`$ cd /var/TKLC/db/filemgmt/`
		
		`#Create backup directory`
		`$mkdir backup`
		
		Verify directory is created:-
		`$ ls -ltr /var/TKLC/db/filemgmt/backup`
		Error should not come "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content.

STEP#	Procedure	Description

3. □	**NOAM/SOAM VIP console:** Change permissions of backup directory	Assuming backup directory is created
		
		Verify directory is created:-
		`$ ls -ltr /var/TKLC/db/filemgmt/backup`
		
		Error should not come "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content.
		
		If directory is not created go back to step 2. Else proceed.
		
		#Change permissions of backup directory
		`$ chmod 770 /var/TKLC/db/filemgmt/backup`
		
		#Change ownership of backup directory
		`$ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup`
		`After changing the permissions and ownership of the backup directory.`
		`Directory will look like`
		`drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15 backup`

4.	**NOAM/SOAM VIP console:** Copy the backup file which we need to restore in backup directory	Copy the backup file to backup directory
		`$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup`
		Provide permissions to backup file inside backup directory.
		# Make sure about present working directory.
		`$cd` **`/var/TKLC/db/filemgmt/backup`**
		
		#Change permissions of files inside backup directory
		`$chmod 666 Backup.*`
		# Change ownership of files inside backup directory
		`$` **`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 will use 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 App server name and IP. Add comma seperated 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 App servers as 'AppServer1', 'AppServer2' etc.
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.

Section	Parameter Name	Description

		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 will be 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 will be in a bad shape for a fresh install. Keeping cleanUpBeforeInstall as "yes" will clean up the server and make 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 App 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`	Provice 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 will be present in this location. This property should not be changed `presentFolder = /u02`

Section	Parameter Name	Description
Files	`targetFolder`	The scripts will be copied to this location. This v should not be changed `targetFolder` = */u03*
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 will be 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 woll create 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*

Section	Parameter Name	Description
		Note: MySQL password will be the default comcol password. It is present in 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 which will be used in all Admin and AppServers nodeManagerUser = *nodemanager* nodeManagerPassword = *tekelec123*
Credentials	nodeManagerPassword	
Credentials	operatorUser	A new operator will be crated with this details to access partner relationship management portal. operatorUser = *oracleop3* operatorPassword = *tekelec123*
Credentials	operatorPassword	
Credentials	adminServerUser	Below is 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 should not be changed, these ports are used only for internal communication adminListenPort = *7001* appListenPort = *8001* appListenPortSSL = *8002*
Ports	adminIMIPorts adminXMIPorts	Ports to be enabled in IP Firewall on Admin server: adminIMIPorts = 7001,5556,7002,9876,8050,3075,9090,7 adminXMIPorts = 9002
Ports	appIMIPorts appXMIPorts appXSIPorts	Ports to be enabled in IP Firewall on AppServers: appIMIPorts = 8001,8002,9876,5556,8050,3075,9090,7 appXMIPorts = 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 below on the Support telephone menu:

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

You will be 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.