Oracle® Database

Oracle Communications Diameter Signaling Router Cloud Disaster Recovery Guide

Release 9.3.0.0.0
G56140-01
May 2026

Oracle Database Oracle Communications Diameter Signaling Router Cloud Disaster Recovery Guide, Release 9.3.0.0.0

G56140-01

Contents

Preface

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

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

Conventions

The following text conventions are used in this document:

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

My Oracle Support

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

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

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

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

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

What's New in this Guide

This section introduces the documentation updates for release 9.3.0.0.0.

Release 9.3.0.0.0 - G56140-01, May 2026

There are no updates for this release.

1 Introduction

This document describes procedures for disaster recovery for Diameter Signaling Router (DSR) (3-tier deployments). This includes recovery of partial or a complete loss of one or more DSR 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. Running this procedure also involves referring to and running procedures in existing support documents.

The components dependent on DSR may need to be recovered as well, for example SDS and IDIH.

> **Note**
>
> Failures may occur from the host or infrastructure level. 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 or Hypervisor related migrations or disaster recovery scenarios are out of scope of this document. This document covers the DR scenarios within the DSR application.

1.1 References

Oracle Communications Diameter Signaling Router Cloud Installation Guide

Oracle Communications Diameter Signaling Router or Subscriber Database Server NOAM Failover Users Guide

Diameter Signaling Router Policy and Charging Application Feature Activation Guide

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1-1 Acronyms

Acronyms	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

Table 1-1 (Cont.) Acronyms

Acronyms	Definition
NOAM	Network Operations, Administration & Maintenance
OS	Operating System
OVA	Open Virtualization Appliance
OVM-M	Oracle Virtual Machine Manager
OVM-S	Oracle Virtual Machine Server
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

1.3 Terminology

Table 1-2 Terminology

Procedure	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 reinstall 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 doesn't provide the hardware or hardware firmware, and isn't responsible for hardware installation, configuration, or maintenance.
Enablement	The business practice of providing support services (hardware, software, documentation, etc) that enables third party entity to install, configure, and maintain Oracle products for Oracle customers.

1.4 Optional Features

Table 1-3 Optional Features

Feature	Document
Diameter Mediation	DSR Cloud installation Procedure

Table 1-3 (Cont.) Optional Features

Feature	Document
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure
Map-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation Procedure
Policy and Charging Application (PCA)	DSR PCA Feature Activation
Host Intrusion Detection System (HIDS)	DSR Security Guide

2 Recovery Scenarios

The DSR disaster recovery procedure falls into six basic categories. It is primarily dependent on the state of the NOAM and SOAM server.

> **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 redeploy base software.

Table 2-1 DSR disaster recovery procedure

Recovery	Servers
Recovery of the entire network from a total outage. See Complete Server Outage (All Servers)	• All NOAM servers failed • All SOAM servers failed • 1 or more MP servers failed
Recovery of one or more servers with at least one NOAM server intact. See Partial Server Outage with One NOAM Server Intact and both SOAMs Failed	• 1 or more NOAM servers intact • All SOAM servers or MP servers failed
Recovery of the NOAM pair with one or more SOAM servers intact. See Partial Server Outage with both NOAM Servers Failed and One SOAM Server Intact	• All NOAM servers failed • 1 or more SOAM servers intact
Recovery of one or more server with at least one NOAM and one SOAM server intact. See Partial Server Outage with NOAM and one SOAM Server Intact	• 1 or more NOAM servers intact • 1 or more SOAM servers intact • 1 or more MP servers failed
Recovery of the NOAM pair with DR-NOAM available and one or more SOAM servers intact. See Partial Server Outage with both NOAM Servers Failed with DR-NOAM Available	• All NOAM servers failed • 1 or more SOAM servers intact • DR-NOAM available
Recovery Scenario 6 Case 1: Recovery of one or more server with corrupt databases that cannot be restored via replication from the active parent node. Case 2: Database Recovery See Partial Service Outage with Corrupt Database	Case 1 • Server is intact. • Database gets corrupted on the server. • Replication is occurring to the server with corrupted database. Case 2 • Server is intact. • Database gets corrupted on the server. • Latest Database backup of the corrupt server is not present. • Replication is inhibited (either manually or because of comcol upgrade barrier).

2.1 Complete Server Outage (All Servers)

Scenarios

- All NOAM servers failed
- All SOAM servers failed
- 1 or more MP servers failed

In the severe case scenario where all the servers in the network have suffered complete software failure. The servers are recovered using OVA images then restoring database backups to the active NOAM and SOAM servers.

Database backups will be taken from customer offsite backup storage locations (assuming these were performed and stored offsite prior to the outage). If no backup files are available, the only option is to rebuild the entire network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually.

2.2 Partial Server Outage with One NOAM Server Intact and both SOAMs Failed

Scenarios

- 1 or more NOAM servers intact.
- All SOAM servers failed.
- 1 or more MP servers failed.

This case assumes that at least one NOAM servers intact. All SOAM servers have failed and are recovered using OVA images. Database is restored on the SOAM server and replication will recover the database of the remaining servers.

2.3 Partial Server Outage with both NOAM Servers Failed and One SOAM Server Intact

Scenarios:

- All NOAM servers failed.
- 1 or more SOAM servers intact.

Database is restored on the NOAM and replication will recover the database of the remaining servers.

2.4 Partial Server Outage with NOAM and one SOAM Server Intact

Scenarios:

- 1 or more NOAM servers intact.
- 1 or more SOAM servers intact.

- 1 or more MP servers failed.

The simplest case of disaster recovery is with at least one NOAM and one SOAM servers intact. All servers are recovered using base recovery of software. Database replication from the active NOAM and SOAM servers will recover the database to all servers.

2.5 Partial Server Outage with both NOAM Servers Failed with DR-NOAM Available

Scenarios:

- All NOAM servers failed.
- 1 or more SOAM servers intact.
- DR-NOAM available.

This case assumes that a partial outage with both NOAM servers failed but a DR NOAM available. The DR NOAM is switched from secondary to primary then recovers the failed NOAM servers.

2.6 Partial Service Outage with Corrupt Database

Case 1: Database is corrupted, replication channel is inhibited (either manually or because of comcol upgrade barrier) and database backup is available.

Case 2: Database is corrupted, but replication channel is active.

3
Procedure Overview

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

3.1 Required Materials

Following are the materials required for disaster recovery:

- Hard copy of all NAPD performed at the initial installation and network configuration of customers site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
- DSR recent backup files: electronic backup file (preferred) or hard copy of all DSR configuration and provisioning data.
- Latest Network Element report: Electronic file or hard copy of Network Element report.
- The network element XML file used for the VMs initial configuration.

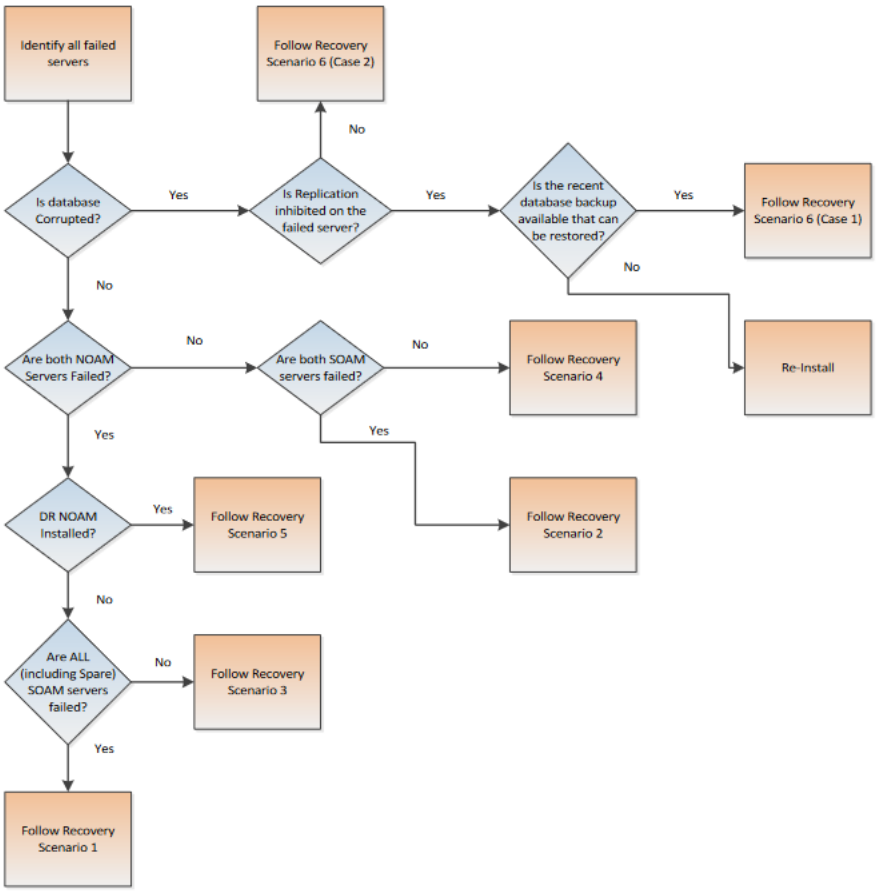
> **Note**
>
> For all Disaster Recovery scenarios, assume that the NOAM and SOAM database backup were performed around the same time, and there are no synchronization issues exist among them.

3.2 Disaster Recovery Strategy

Disaster recovery procedure is performed as part of a disaster recovery strategy with the basic steps listed below:

- Evaluate failure conditions in the network and determine that normal operations cannot continue without disaster recovery procedure. This means the failure conditions in the network match one of the failure scenarios described in Recovery Scenarios
- Read and review the content in this document.
- Gather Required Materials.
- Use figure 3-1 to identify the recovery scenario and procedure to follow based on the failure conditions.
- Run appropriate recovery procedures as mentioned in the Recovering and Restoring System Configuration.

Figure 3-1 Determining Recovery Scenario



4 Disaster Recovery Procedure

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

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

> **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 the Oracle Support assessment of Disaster, it may require to deviate from the documented process.

4.1 Recovering and Restoring System Configuration

Disaster recovery requires configuring the system as it was before the disaster and restoration of operational information. There are 8 distinct procedures to choose from depending on the type of recovery needed. Only one of these must be followed.

> **Warning**
>
> - Whenever there is a need to restore the database backup for NOAM and SOAM 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, refer Workarounds for Issues not fixed in this Release this will provide steps to check and create the backup directory.
> - Following is the standard file format to be used for recovery. `Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2`

4.1.1 Recovery Scenario 1 (Complete Server Outage)

For a complete server outage, NOAM servers are recovered using recovery procedures for software and then running a database restore to the active NOAM server. 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. This list will help to understand the recovery procedure summary. Do not use this list to run the procedure. The major activities are summarized as follows.

Recover Base software for all VMs:

- Recover the Standby NOAM server by recovering base software, for a Non-HA deployment this can be skipped.

  - Reconfigure the DSR Application.
- Recover all SOAM and MP servers by recovering software, In a Non-HA deployment the standby or spare SOAM servers can be skipped.
  - Recover the SOAM database.
  - Reconfigure the DSR Application.
  - Reconfigure the signaling interface and routes on the MPs, the DSR software will automatically reconfigure the signaling interface from the recovered database.

Restart process and re-enable provisioning replication

> **Note**
>
> Any other applications DR recovery actions (SDS and IDIH) may occur in parallel. These actions must be worked simultaneously, doing so would allow faster recovery of the complete solution (i.e. stale DB on DP servers will not receive updates until SDS-SOAM servers are recovered.

This procedure performs recovery if both NOAM servers are failed and all SOAM servers are failed. This procedure also covers the C-Level server failure.

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.

Perform the following procedure for recovery:

1. Refer Workarounds for Issues not fixed in this Release to understand or apply any workarounds required during this procedure.
2. Gather the documents and required materials listed in the Required Materials section.
3. Recover the failed software:
   VMware based deployments:
   a. For NOAMs run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure NOAM guests based on resource profile.
   b. For SOAMs run the following procedures:
      i. Import DSR OVA

> **Note**
>
> If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

ii. Configure Remaining DSR guests based on resource profile

c. For failed MPs run the following procedures:

i. Import DSR OVA.

> **Note**
>
> If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

ii. Configure remaining DSR guests based on resource profile.

d. For KVM or Openstack based deployments:

i. Import DSR OVA.

> **Note**
>
> If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

ii. Configure NOAM guests based on resource profile.

e. For SOAMs run the following procedures:

i. Import DSR OVA.

> **Note**
>
> If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

ii. Configure remaining DSR guests based on resource profile.

f. For OVM-S/OVM-M based deployments run the following procedures:

i. Import DSR OVA and prepare for VM creation.

ii. Configure each DSR VM.

> **Note**
>
> While running procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs). For more information, see *Oracle Communications Diameter Signaling Router Cloud installation Guide*.

.

4. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.

a. From Required Materials list, use site survey documents and Network Element report (if available), to determine network configuration data.

5. Run DSR installation procedure for the first NOAM:
   a. Verify the networking data for Network Elements.

> **Note**
>
> Use the backup copy of network configuration data and site surveys.

   b. Run installation procedures for the first NOAM server:
      i. Configure the First NOAM NE and Server.
      ii. Configure the NOAM Server Group.
6. Log in to the NOAM GUI as the guiadmin user.
7. Navigate to **Main Menu**, and then **Status & Manage**, and then **Files**.
   a. Select the **Active NOAM** server and click **Upload**.
   b. Select "NO Provisioning and Configuration" file, backed up after initial installation and provisioning.
   c. Click **Browse** and locate the backup file.
   d. Check **This is a backup file** box and click **Upload**.
   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.
8. To disable provisioning:
   a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
   b. click **Disable Provisioning**. A confirmation window will appear, press **OK** to disable.

> **Note**
>
> The message "warning Code 002" will appear.

9. Verify the archive contents and database compatibility:
   a. Select the **Active NOAM** server and click **Compare**.
   Click **restored database** file that was uploaded as a part of step 13 of this procedure.
   b. Verify that the output window matches the database.

> **Note**
>
> - As expected, the user will see a database mismatch with respect to the VMs NodeIDs. Proceed if this is the only difference, if not, contact My Oracle Support (MOS).
> - Archive content and database compatibilities must consist the following:
>   - Archive Contents: Configuration data
>   - Database Compatibility: The databases are compatible.
> - When restoring from an existing backup database to a database using a single NOAM, the expected outcome for the topology compatibility check is as follows:
>   - Topology compatibility: Topology must be compatible minus the NODEID.
> - Attempting to restore a backed-up database onto a NOAM database which is empty. In the context of Topology Compatibility, this text is expected.
>
> If the verification is successful, click **Back** and continue to next step of this procedure.

10. Restore the database:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Select the **Active NOAM** server and click **Restore**. Select the appropriate backup provisioning and configuration file and click **OK**.

> **Note**
>
> As expected, the user will see a database mismatch with respect to the VMs NodeIDs. Proceed if this is the only difference, if not, contact My Oracle Support (MOS).

    c. Select the **Force** checkbox and click **OK** to proceed with the database restore.

> **Note**
>
> After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.

11. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`.
12. Monitor and confirm database restoral. Wait for 5 to10 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:

a. 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.
> - The maintenance and configuration data will be in the same state as when it was first backed up.

13. Log in to the recovered Active NOAM through SSH terminal as admusr user.
14. Recover Standby NOAM:
    a. Install the second NOAM server by running the following procedures:
        i. "Configure the Second NOAM server" steps 1, 3, and 7.
        ii. "Complete Configuring the NOAM Server Group " step 4.
15. Correct the recognized authority table:
    a. Establish an SSH session to the active NOAM, log in as an admusr.
    b. Run 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. Restart DSR application:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
    b. Select the recovered standby NOAM server and click **Restart**.
17. Set HA on Standby NOAM:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    b. Click **Edit**, select the standby NOAM server and set it to **Active** and click **OK**.
18. Perform key exchange with Export Server:
    a. Navigate to **Main Menu**, **Administration**, **Remote Servers** and then **Data Export**.
    b. Click **SSH Key Exchange**, enter the password and click **OK**.
19. Replication will wipe out the databases on the C-Level servers when Active SOAM is recovered, hence prevent replication to the operational C-Level servers that are part of the same site as the failed SOAM servers.

> **Warning**
>
> - If the spare SOAM is also present in the site and lost: Inhibit A and B level replication on C-Level servers (when Active, Standby, and Spare SOAMs are lost)
> - If the spare SOAM is not deployed in the site: Run Inhibit A and B level replication on C-Level servers.

20. Run the steps 1 and 3 to 7 "Configure the SOAM Servers" to install the SOAM servers.

> **Note**
>
> Before continuing to next step, wait for the server to restart.

21. Restart DSR application on recovered Active SOAM Server:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
    b. Select the recovered server and click **Restart**.
22. Upload the backed up SOAM database file:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Files**.
    b. Select the Active SOAM server. Click **Upload** and select the file "SOAM Provisioning and Configuration" backed up after initial installation and provisioning.
    c. Click **Browse** and locate the backup file.
    d. Check **This is a backup file** box and click **Open**.
    e. Click **Upload**.
    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.
23. Establish a GUI session on the recovered SOAM server. Open the web browser and enter the following url `http://<Recovered_SOAM_IP_Address>`.
24. Recovered SOAM GUI, verify the archive contents and database compatibility:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Select the Active SOAM server and click **Compare**.
    c. Click **Restored Database** file that was uploaded as a part of step 13 of this procedure. Verify that the output window matches the database archive.

> **Note**
>
> - As expected, the user will see a database mismatch with respect to the VMs NodeIDs. Proceed if this is the only difference, if not, contact My Oracle Support (MOS).
> - Archive content and database compatibilities must consist the following:
>   - Archive Contents: Configuration data
>   - Database Compatibility: The databases are compatible.
> - When restoring from an existing backup database to a database using a single NOAM, the expected outcome for the topology compatibility check is as follows:
>   - Topology compatibility: Topology must be compatible minus the NODEID.
> - Attempting to restore a backed-up database onto a NOAM database which is empty. In the context of Topology Compatibility, this text is expected.
>
> If the verification is successful, click **Back** and continue to next step of this procedure.

25. Restore the Database:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Select the **Active NOAM** server and click **Restore**. Select the appropriate backup provisioning and configuration file and click **OK**.

> **Note**
>
> As expected, the user will see a database mismatch with respect to the VMs NodeIDs. Proceed if this is the only difference, if not, contact My Oracle Support (MOS).

    c. Select the **Force** checkbox and click **OK** to proceed with the database restore.

> **Note**
>
> After the restore has started, the user will be logged out of **XMI NO GUI** since the restored topology is old data.

26. 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.

> **Note**
>
> - Do not pay attention to alarms until all the servers in the system are completely restored.
> - The maintenance and configuration data will be in the same state as when it was first backed up.

27. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`.
28. Recover remaining SOAM Server:
    a. Install the SOAM servers by running the following procedure:
        i. Run the steps 1 and 3 to 6 "Configure the SOAM Servers" to Install the SOAM servers.

> **Note**
>
> Before continuing to next step, wait for the server to reboot.

29. Restart DSR application on remaining SOAM Server(s):
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
    b. Select the recovered server and click **Restart**.
30. Set HA on recovered standby SOAM server:

> **Note**
>
> For Non-HA sites, skip this step.

    a. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    b. Click **Edit** and set "Max Allowed HA Role" to **Active** and click **OK**.
31. Start replication on working C-Level servers:
    Un-Inhibit (Start) replication to the working C-Level servers which belong to the same site as of the failed SOAM servers.

    If the spare SOAM is also present in the site and lost: run un-inhibit A and B level replication on C-level servers (when Active, Standby and Spare SOAMs are lost).

    If the spare SOAM is not deployed in the site: run un-inhibit A and B Level replication on C-level servers.

    Navigate to **Main Menu**, **Status & Manage**, and then **Database**.

    If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using the following order, if none of the servers are inhibited, skip this step and continue with the next step:

    - Active NOAM Server
    - Standby NOAM Server
    - Active SOAM Server
    - Standby SOAM Server

- Spare SOAM Server (if applicable)
- MP/IPFE Servers
- SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare)

Verify that the replication on all the working servers is allowed.

32. Establish a SSH session to the C-Level server being recovered, login as an admusr.
    a. Run the following command to set shared memory to unlimited:

       ```
       $ sudo shl.set –m 0
       ```

    b. Run the following step from each server that has been recovered:
        i. Run the steps 1, 11 to 14 (step 15 if required) configure the MP Virtual Machines.
33. Restart DSR application for recovered C- Level server:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
    b. Select the recovered server and click **Restart**.
34. Start replication on all C-Level servers:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. If the **Repl status** is set to **Inhibited**, click **Allow Replication** by following the order:
        i. Active NOAM Server
        ii. Standby NOAM Server
        iii. Active SOAM Server
        iv. Standby SOAM Server
        v. Spare SOAM Server (if applicable)
        vi. MP/IPFE Servers
    c. Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status.
35. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    a. Click **Edit**, for each server whose "Max Allowed HA Role" is set to **OOS**, set it to **Active** and click **OK**.
36. Perform key exchange between the Active-NOAM and recovered servers:
    a. Establish an SSH session to the Active NOAM, log in as an admusr.
    b. Run the following command to perform a key exchange from the Active NOAM to each recovered server:

       ```
       $ keyexchange admusr@<Recovered Server Hostname>
       ```

       > **Note**
       >
       > Perform this step, If an export server is configured.

37. Activate optional features:
    a. Establish an SSH session to the Active NOAM, log in as admusr.

> **Note**
>
> - If PCA is installed in the system that is being recovered, perform the following procedures on all the active applications:
>   - PCA Activation on Standby NOAM on recovered Standby NOAM server
>   - PCA Activation on Active SOAM on recovered Active SOAM Server from to re-activate PCA
>
>   For more information about the above mentioned procedures, see *Diameter Signaling Router Policy and Charging Application User Guide.*

Refer Optional Features to activate any features that were previously activated.

> **Note**
>
> - While running the activation script, the following error message (and corresponding messages) output may be seen, the error can be ignored `iload#31000{S/W Fault}`.
> - If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.

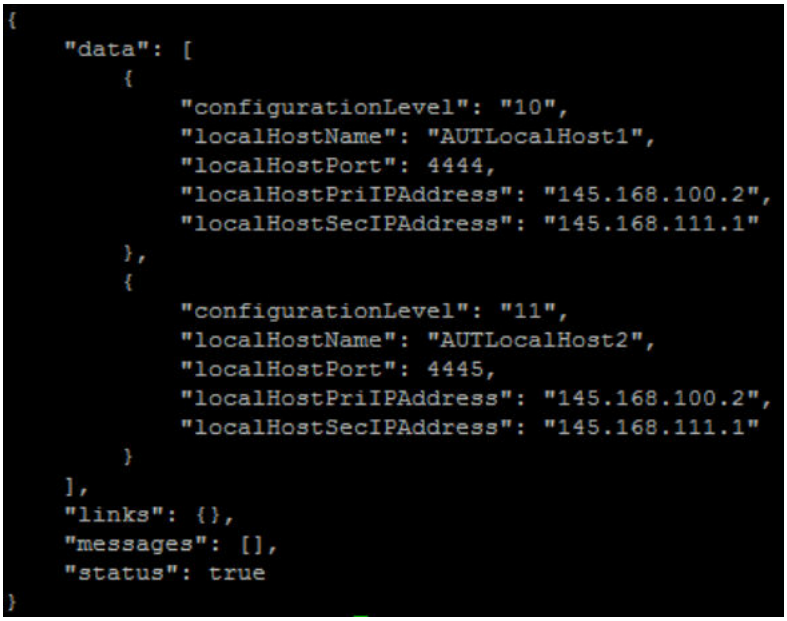
38. Fetch and store the database report for the newly restored data and save it:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Select the Active NOAM server and click **Report**.
    c. Click **Save** and save the report to the local machine.
39. Verify replication between servers:
    a. Log in to the Active NOAM through SSH terminal as admusr user.
    b. Run the following command:

```
$ sudo irepstat –m
Output like below shall be generated:
-- Policy 0 ActStb [DbReplication] ---------------------
Oahu-DAMP-1 -- Active
BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me
CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A=me
Oahu-DAMP-2 -- Stby
BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s A=C3642.212
CC From Oahu-DAMP-1 Active 0 0.10 ^0.14 1.16%cpu 31B/s
A=C3642.212
Oahu-IPFE-1 -- Active
BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s A=C3642.212
Oahu-IPFE-2 -- Active
BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212
Oahu-NOAM-1 -- Stby
AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s
Oahu-NOAM-2 -- Active
AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s
```

```
AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s
Oahu-SOAM-1 -- Stby
BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s
Oahu-SOAM-2 -- Active
AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s
BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s
BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s
irepstat ( 40 lines) (h)elp (m)erged
```

40. Verify the database states:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Verify that the "OAM Max HA Role" is either **Active** or **Standby** for NOAM and SOAM and "Application Max HA Role" for MPs is **Active**, and that the status is **Normal**.
41. Verify the HA Status:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    b. Select the row for all of the servers, verify that the **HA** role is either **Active** or **Standby**.
42. Enable Provisioning:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Click **Enable Provisioning**. A confirmation window will appear, click **OK** to enable Provisioning.
43. Verify the local node Info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Connections**.
    b. Verify that all the connections are shown.
44. Verify the peer node info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Peer Nodes**.
    b. Verify that all the peer nodes are shown.
45. Verify the connections info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Connections**.
    b. Verify that all the connections are shown.
46. To verify the vSTP MP local nodes info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command `[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts`
    c. Verify if the output is similar to the following output.

Figure 4-1 Output



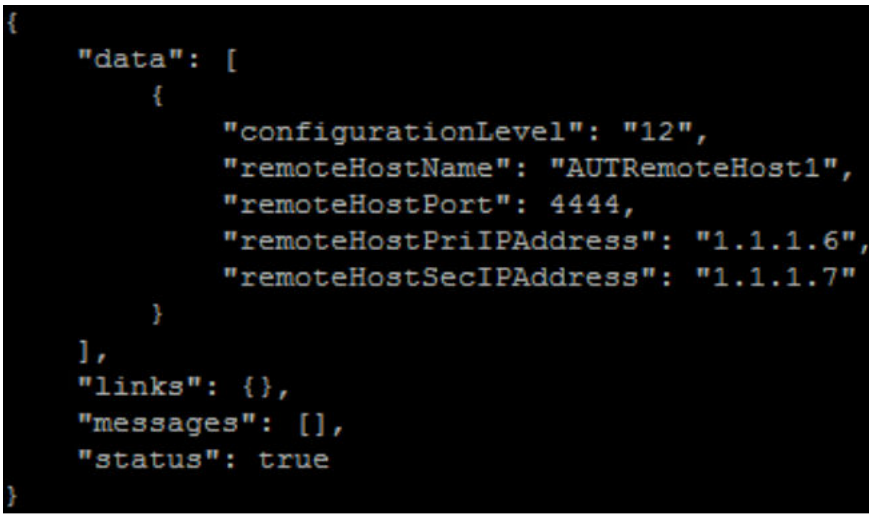
```
{
    "data": [
        {
            "configurationLevel": "10",
            "localHostName": "AUTLocalHost1",
            "localHostPort": 4444,
            "localHostPriIPAddress": "145.168.100.2",
            "localHostSecIPAddress": "145.168.111.1"
        },
        {
            "configurationLevel": "11",
            "localHostName": "AUTLocalHost2",
            "localHostPort": 4445,
            "localHostPriIPAddress": "145.168.100.2",
            "localHostSecIPAddress": "145.168.111.1"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```


47. To verify the vSTP MP remote nodes info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command:

    ```
    [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
    ```

    c. Verify if the output is similar to the following output:

Figure 4-2 Output



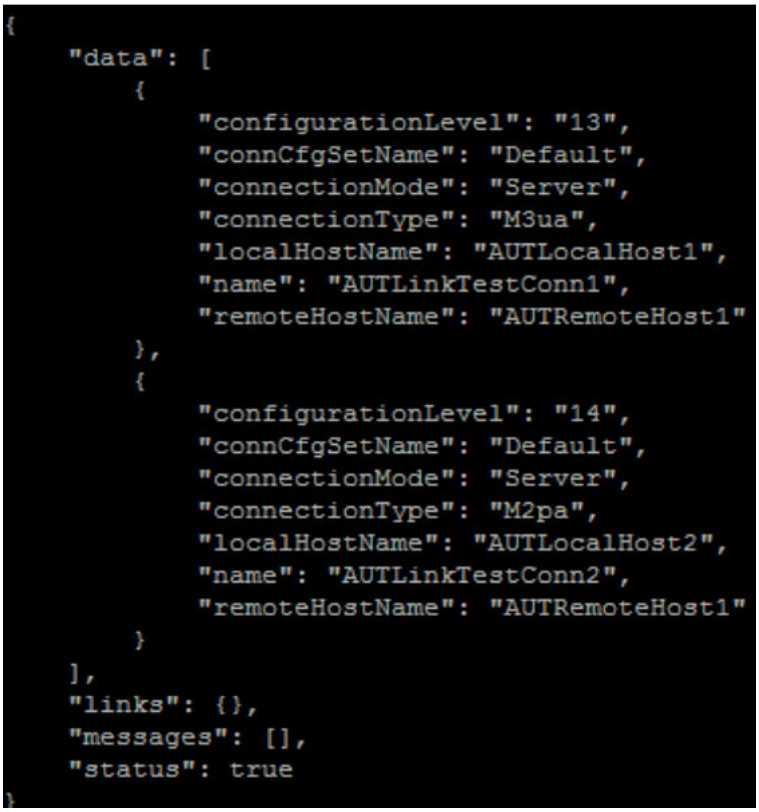
```
{
    "data": [
        {
            "configurationLevel": "12",
            "remoteHostName": "AUTRemoteHost1",
            "remoteHostPort": 4444,
            "remoteHostPriIPAddress": "1.1.1.6",
            "remoteHostSecIPAddress": "1.1.1.7"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```


48. To verify the vSTP MP connections info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command:

    ```
    [admusr@SOAM1 ~]$ mmiclient.py /vstp/connections
    ```

c. Verify if the output is similar to the following output:

Figure 4-3 Output



49. Disable SCTP auth flag:
    a. For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix.
    b. Run this procedure on all Failed MP Servers.
50. Enable connections if needed:
    a. Navigate to **Main Menu**, **Diameter**, **Maintenance**, and then **Connections**.
    b. Select each connection and click **Enable**. Alternatively you can enable all the connections by selecting **EnableAll**.
    c. Verify that the "Operational State" is **Available**.

> **Note**
>
> If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.

51. Enable Optional Features:
    a. Navigate to **Main Menu**, **Diameter**, **Maintenance**, and then **Applications**.
    b. Select the optional feature application configured before and click **Enable**.
52. If required, re-enable transport:

a. Navigate to **Main Menu**, **Transport Manager**, **Maintenance**, and then **Transport**.
b. Select each transport and click **Enable**.
c. Verify that the operational status for each transport is up.

53. Re-enable MAPIWF application if needed:
    a. Navigate to **Main Menu**, **Sigtran**, **Maintenance**, and then **Local SCCP Users**.
    b. Click **Enable** corresponding to MAPIWF application Name.
    c. Verify that the SSN status is **Enabled**.
54. Re-enable links if needed.
    a. Navigate to **Main Menu**, **Sigtran**, **Maintenance**, and then **Links**.
    b. Click **Enable** for each link.
    c. Verify that the operational status for each link is up.
55. Examine All Alarms:
    a. Navigate to **Main Menu**, **Alarms & Events** and **View Active**.
    b. Examine all active alarms and refer to the on-line help on how to address them. For any queries contact My Oracle Support (MOS).
56. Restore GUI usernames and passwords:
    a. If applicable, run steps in section 6.0 to recover the user and group information restored.
57. Backup and archive all the databases from the recovered system:
    a. Run DSR database backup to back up the configuration databases.

4.1.2 Recovery Scenario 2 Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed

For a partial server outage with NOAM server intact and available, SOAM servers are recovered using recovery procedures for software and then running a database restore to the Active SOAM server using a database backup file obtained from the SOAM servers. 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 run the procedure. The major activities are summarized as follows:

Recover Standby NOAM server (if needed) by recovering software and the database.

- Recover the Database.

Recover any failed SOAM and MP servers by recovering software.

- Recover the software.
- The database has already been restored at the Active SOAM server and does not require restoration at the SO and MP servers.

Perform the following procedure for recovery if at least 1 NOAM server is available but all SOAM servers in a site have failed. This includes any SOAM server that is in another location:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS)

1. Refer Workarounds for Issues not fixed in this Release to understand or apply any workarounds required during this procedure.
2. Gather the documents and required materials listed in the Required Materials section.
3. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`.
4. Set failed servers to OOS:
   a. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
   b. Click **Edit**, set the "Max Allowed HA" role server to OOS for the failed servers and click **OK**.
5. Create VMs recover the failed software:
   VMware based deployments:
   a. For NOAMs run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure NOAM guests based on resource profile.
   b. For SOAMs run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure remaining DSR guests based on resource profile
   c. For failed MPs run the following procedures:
      i. Import DSR OVA.

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

      ii. Configure Remaining DSR guests based on resource profile.
   d. For NOAMs run the following procedures:
      i. Import DSR OVA.

> **Note**
>
> If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

ii. Configure NOAM guests based on resource profile.

e. For SOAMs run the following procedures:

i. Import DSR OVA.

> **Note**
>
> If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

ii. Configure remaining DSR guests based on resource profile.

f. For OVM-S/OVM-M based deployments run the following procedures:

i. Import DSR OVA and prepare for VM creation.

ii. Configure each DSR VM.

> **Note**
>
> While running procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs). For more information, see *Diameter Signaling Router Cloud Installation Guide*.

6. If required, repeat step 5 for all remaining failed servers.
7. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`.
8. Install the second NOAM server by running the following procedures:
   a. Run step 1 and 3 to 7 of "Configure the Second NOAM server".
   b. Run step 4 of "Complete Configuring the NOAM server".

> **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.

9. Restart DSR application
   a. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
   b. Select the recovered standby NOAM server and click **Restart**.
10. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    a. Click **Edit**, select the standby NOAM server, set it to Active and click **OK**.

11. Replication will wipe out the databases on the C-Level servers when Active SOAM is recovered, hence prevent replication to the operational C-Level servers that are part of the same site as the failed SOAM servers.

> **Warning**
>
> - If the spare SOAM is also present in the site and lost: Inhibit A and B level replication on C-Level servers (when Active, Standby, and Spare SOAMs are lost)
> - If the spare SOAM is not deployed in the site: run Inhibit A and B level replication on C-Level servers.

12. Install the SOAM servers by running the following procedure:
    a. Run steps 1 and 3 to 7 to configure the SOAM servers.

> **Note**
>
> Before continuing to next step, wait for the server to reboot.

13. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    a. Click **Edit**, select the standby NOAM server, set it to **Active** and click **OK**.
14. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
    a. Select the recovered Active SOAM server and click **Restart**.
15. Upload the backed up SOAM Database file:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Files**.
    b. Select the Active SOAM server and click **Upload**.
    c. Select the file "NO Provisioning and Configuration" file backed up after initial installation and provisioning.
        i. Click **Browse** and locate the backup file.
        ii. Check **This is a backup file** box.
        iii. Click **Open** and click **Upload**.
        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
16. Establish a GUI session on the recovered SOAM server. Open the web browser and enter the following url `http://<Recovered_SOAM_IP_Address>`.
17. Recovered SOAM GUI, verify the archive contents and database compatibility:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Select the Active SOAM server and click **Compare**.
    c. Click **Restored Database** file that was uploaded as a part of step 14 of this procedure. Verify that the output window matches the database archive.

> **Note**
>
> - As expected, the user will see a database mismatch with respect to the VMs NodeIDs. Proceed if this is the only difference, if not, contact My Oracle Support (MOS).
> - Archive content and database compatibilities must consist the following:
>   - Archive Contents: Configuration data
>   - Database Compatibility: The databases are compatible.
> - When restoring from an existing backup database to a database using a single NOAM, the expected outcome for the topology compatibility check is as follows:
>   - Topology compatibility: Topology must be compatible minus the NODEID.
> - Attempting to restore a backed-up database onto a NOAM database which is empty. In the context of Topology Compatibility, this text is expected.
>
> If the verification is successful, click **Back** and continue to next step of this procedure.

18. Restore the Database:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Select the **Active NOAM** server and click **Restore**. Select the appropriate backup provisioning and configuration file and click **OK**.

> **Note**
>
> As expected, the user will see a database mismatch with respect to the VMs NodeIDs. Proceed if this is the only difference, if not, contact My Oracle Support (MOS).

    c. Select the **Force** checkbox and click **OK** to proceed with the database restore.

> **Note**
>
> After the restore has started, the user will be logged out of **XMI NO GUI** since the restored Topology is old data. The provisioning will be disabled after this step.

19. 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.

> **Note**
>
> - Do not pay attention to alarms until all the servers in the system are completely restored.
> - The maintenance and configuration data will be in the same state as when it was first backed up.

20. Install the SOAM servers by running the following procedure:
    a. Run step 1 and 3 to 6 "Configure the SOAM Servers" to install the SOAM servers.

    > **Note**
    >
    > Before continuing to next step, wait for the server to reboot.

21. Un-Inhibit (Start) replication to the recovered SOAM servers:
    a. Navigate to **Main Menu**, and then **Status & Manage**, and then **Database**.
    b. Click **Allow Replication** on the recovered SOAM servers.
    c. Verify that the replication on all SOAMs servers is allowed. This can be done by checking "Repl" status column of respective server.
22. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
23. When prompted "Are you sure you wish to Force an NTP Sync on the following server(s)? SOAM2, click **OK**.
24. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    a. Click **Edit**, For each SOAM server whose "Max Allowed HA" role is set to **Standby**, set it to **Active**.
25. Navigate to **Main Menu**, **Status & Manage**, and then **Server**. Select the recovered server and click **Restart**.
26. Enable Provisioning:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Click **Enable Site Provisioning**, a confirmation window will appear, click **OK** to enable Provisioning.
27. Un-Inhibit (Start) replication to the working C Level servers which belong to the same site as of the failed SOAM servers.
    If the spare SOAM is also present in the site and lost: run un-inhibit A and B level replication on C-Level servers (when Active, Standby and Spare SOAMs are lost).

    If the spare SOAM is not deployed in the site: run un-inhibit A and B level replication on C-Level servers.

    Navigate to **Main Menu**, **Status & Manage**, and then **Database**.

    If the "Repl Status" is set to **Inhibited**, click **Allow Replication** using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step:

    - Active NOAM Server
    - Standby NOAM Server
    - Active SOAM Server

- Standby SOAM Server
- Spare SOAM Server (if applicable)
- MP/IPFE Servers
- SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare.)

Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table.

28. Establish a SSH session to the C level server being recovered, login as an admusr.
    a. Run the following command to set shared memory to unlimited

       ```
       $ sudo shl.set –m 0
       ```

    b. Run the following procedures for each server that has been recovered:
        i. Run step 1, 8 to 14, (step 15 if required) configure the MP Virtual Machines.
29. Start replication on all C-Level servers:
    a. Navigate to **Main Menu**, and then **Status & Manage**, and then **Database**.
    b. If the "Repl" status is set to **Inhibited**, click **Allow Replication** by following the order:
        i. Active NOAM Server
        ii. Standby NOAM Server
        iii. Active SOAM Server
        iv. Standby SOAM Server
        v. Spare SOAM Server (if applicable)
        vi. MP/IPFE Servers
    c. Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table.
30. Perform key exchange between the Active NOAM and recovered servers:
    a. Establish an SSH session to the Active NOAM, log in as an admusr.
    b. Run the following command to perform a key exchange from the Active NOAM to each recovered server:

       ```
       $ keyexchange admusr@<Recovered Server Hostname>
       ```

       > **Note**
       >
       > Perform this step, if an export server is configured.

31. Activate optional features:
    a. Establish an SSH session to the active NOAM, log in as admusr.

> **Note**
>
> - If PCA is installed in the system that is being recovered, perform the following procedures on all the active applications:
>   - PCA Activation on Standby NOAM on recovered Standby NOAM server
>   - PCA Activation on Active SOAM on recovered Active SOAM Server from to re-activate PCA
>
>   For more information about the above mentioned procedures, see *Diameter Signaling Router Policy and Charging Application User Guide.*

Refer Optional Features to activate any features that were previously activated.

> **Note**
>
> - While running the activation script, the following error message (and corresponding messages) output may be seen, the error can be ignored `iload#31000{S/W Fault}`.
> - If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.

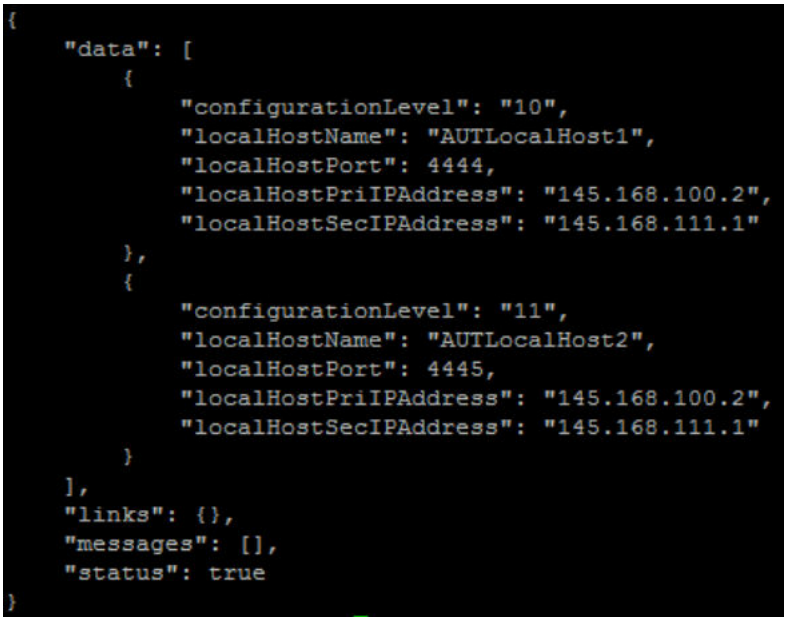
32. Fetch and store the database report for the newly restored data and save it:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Select the Active NOAM server and click **Report**.
    c. Click **Save** and save the report to the local machine.
33. Verify replication between servers:
    a. Log in to the Active NOAM through SSH terminal as admusr user.
    b. Run the following command:

```
$ sudo irepstat –m
Output like below shall be generated:
-- Policy 0 ActStb [DbReplication] ---------------------
Oahu-DAMP-1 -- Active
BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me
CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A=me
Oahu-DAMP-2 -- Stby
BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s A=C3642.212
CC From Oahu-DAMP-1 Active 0 0.10 ^0.14 1.16%cpu 31B/s
A=C3642.212
Oahu-IPFE-1 -- Active
BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s A=C3642.212
Oahu-IPFE-2 -- Active
BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212
Oahu-NOAM-1 -- Stby
AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s
Oahu-NOAM-2 -- Active
AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s
```

```
AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s
Oahu-SOAM-1 -- Stby
BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s
Oahu-SOAM-2 -- Active
AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s
BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s
BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s
irepstat ( 40 lines) (h)elp (m)erged
```

34. Verify the database states:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Verify that the "OAM Max HA Role" is either **Active** or **Standby** for NOAM and SOAM and "Application Max HA Role" for MPs is **Active**, and that the status is **Normal**.
35. Verify the HA Status:
    a. Navigate to **Main Menu**, and then **Status & Manage**, and then **HA**.
    b. Select the row for all of the servers, verify that the **HA** role is either **Active** or **Standby**.
36. Verify the local Node Info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Connections**.
    b. Verify that all the connections are shown.
37. Verify the Peer Node Info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Peer Nodes**.
    b. Verify that all the peer nodes are shown.
38. Verify the Connections Info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Connections**.
    b. Verify that all the connections are shown.
39. To verify the vSTP MP Local nodes info:
    a. Log in to the SOAM VIP Server console as admusr.
    b. Run the following command `[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts`
    c. Verify the output similar to the below output.

Figure 4-4 Output



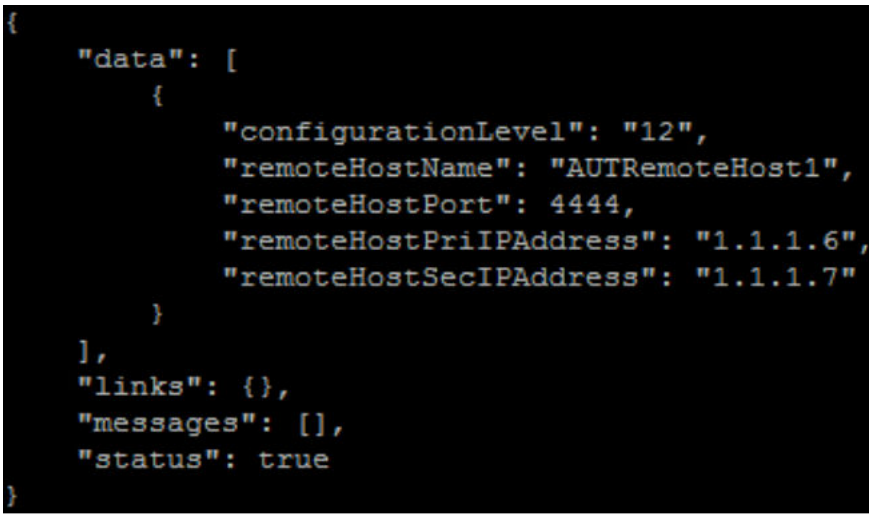
```
{
    "data": [
        {
            "configurationLevel": "10",
            "localHostName": "AUTLocalHost1",
            "localHostPort": 4444,
            "localHostPriIPAddress": "145.168.100.2",
            "localHostSecIPAddress": "145.168.111.1"
        },
        {
            "configurationLevel": "11",
            "localHostName": "AUTLocalHost2",
            "localHostPort": 4445,
            "localHostPriIPAddress": "145.168.100.2",
            "localHostSecIPAddress": "145.168.111.1"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```


40. To verify the vSTP MP remote nodes info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command:

    ```
    [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
    ```

    c. Verify the output similar to the below output:

Figure 4-5 Output



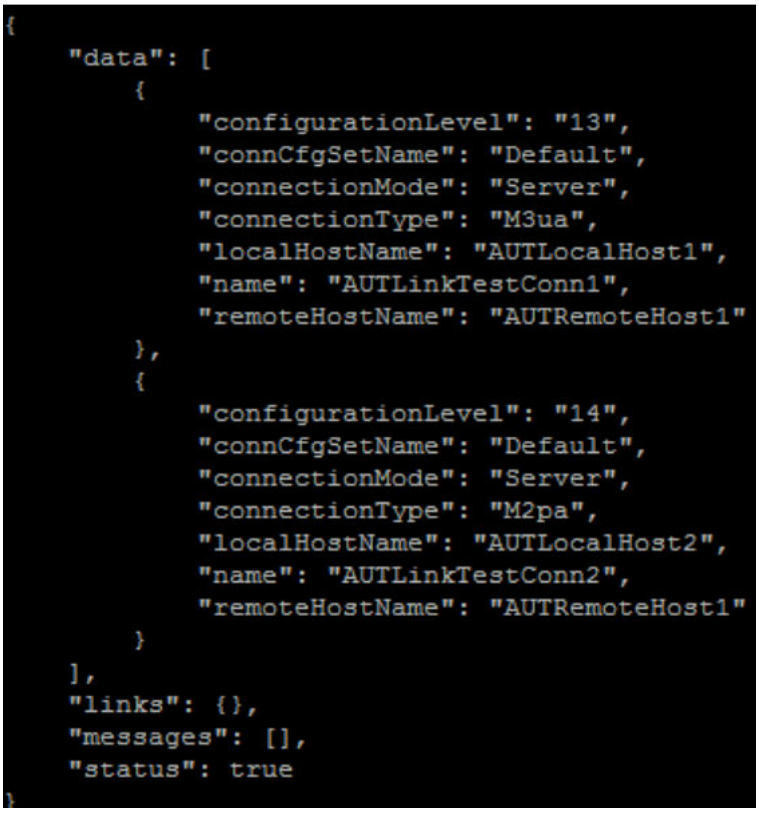
```
{
    "data": [
        {
            "configurationLevel": "12",
            "remoteHostName": "AUTRemoteHost1",
            "remoteHostPort": 4444,
            "remoteHostPriIPAddress": "1.1.1.6",
            "remoteHostSecIPAddress": "1.1.1.7"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```


41. To verify the vSTP MP Connections info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command:

    ```
    [admusr@SOAM1 ~]$ mmiclient.py /vstp/connections
    ```

c. Verify if the output is similar to the below output:

Figure 4-6 Output



42. Disable SCTP Auth Flag:
    a. For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS.
    b. Run this procedure on all failed MP Servers.
43. Enable Connections if needed:
    a. Navigate to **Main Menu**, **Diameter**, **Maintenance**, and then **Connections**.
    b. Select each connection and click **Enable**. Alternatively you can enable all the connections by selecting **EnableAll**.
    c. Verify that the "Operational State" is **Available**.
44. Enable Optional Features:
    a. Navigate to **Main Menu**, **Diameter**, **Maintenance**, and then **Applications**.
    b. Select the optional feature application configured in step 29 and click **Enable**.
45. If required, re-enable transport:
    a. Navigate to **Main Menu**, **Transport Manager**, **Maintenance**, and then **Transport**.
    b. Select each transport and click **Enable**.
    c. Verify that the operational status for each transport is up.
46. Re-enable MAPIWF application if needed:
    a. Navigate to **Main Menu**, **Sigtran**, **Maintenance**, and then **Local SCCP Users**.

b. Click **Enable** corresponding to MAPIWF application Name.

c. Verify that the SSN status is **Enabled**.

47. Re-enable links if needed.

a. Navigate to **Main Menu**, **Sigtran**, **Maintenance**, and then **Links**.

b. Click **Enable** for each link.

c. Verify that the operational status for each link is up.

48. Examine All Alarms:

a. Navigate to **Main Menu**, **Alarms & Events** and **View Active**.

b. Examine all active alarms and refer to the on-line help on how to address them. For any queries contact My Oracle Support (MOS).

49. Backup and archive all the databases from the recovered system:

a. Run DSR database backup to back up the configuration databases.

4.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)

For a partial server outage with SOAM server intact and available, NOAM servers are recovered using recovery procedures for software and then running a database restore to the active NOAM server using a NOAM database backup file obtained from external backup sources such as customer servers. All other servers are recovered using recovery procedures for software. Database replication from the Active NOAM or Active SOAM 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 run the procedure. The major activities are summarized as follows:

Recover Active NOAM server by recovering software and the database.

- Recover the software.
- Recover the database

Recover standby NOAM servers by recovering software.

- Recover the software.

Recover any failed SOAM and MP servers by recovering software.

- Recover the software.
- Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP servers.

Perform the following procedure for recovery if all NOAM servers are failed but 1 or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server):

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.

1. Refer Workarounds for Issues not fixed in this Release to understand or apply any workarounds required during this procedure.

2. Gather the documents and required materials listed in the Required Materials section.
3. VMware based deployments:
   a. For NOAMs run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure NOAM guests based on resource profile.
   b. For SOAM run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure remaining DSR guests based on resource profile
   c. For failed MPs run the following procedures:
      i. Import DSR OVA.

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

      ii. Configure remaining DSR guests based on resource profile.
   d. For NOAMs run the following procedures:
      i. Import DSR OVA.

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

      ii. Configure NOAM guests based on resource profile.
   e. For SOAM run the following procedures:
      i. Import DSR OVA.

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

ii. Configure remaining DSR guests based on resource profile.

f. For OVM-S/OVM-M based deployments run the following procedures:

i. Import DSR OVA and prepare for VM creation.

ii. Configure each DSR VM.

> **Note**
>
> While running procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs). For more information, see *Diameter Signaling Router Cloud Installation Guide*.

4. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.

a. From Required Materials list, use site survey documents and Network Element report (if available), to determine network configuration data.

5. Run DSR installation procedure for the first NOAM:

a. Verify the networking data for Network Elements.

> **Note**
>
> Use the backup copy of network configuration data and site surveys.

b. Run installation procedures for the first NOAM server:

i. Configure the first NOAM NE and Server.

ii. Configure the NOAM Server Group.

6. Log in to the NOAM GUI as the guiadmin user.

7. Upload the backed up SOAM database file:

a. Navigate to **Main Menu**, **Status & Manage**, and then **Files**.

b. Select the Active SOAM server. Click **Upload** and select the file "SO Provisioning and Configuration" backed up after initial installation and provisioning.

c. Click **Browse** and locate the backup file.

d. Check **This is a backup file** box and click **Open**.

e. Click **Upload**.
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.

8. To disable provisioning:

a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.

b. Click **Disable Provisioning**. A confirmation window will appear, press **OK**to disable.

> **Note**
>
> The message "warning Code 002" will appear.

9. Verify the archive contents and database compatibility:

a. Select the **Active NOAM** server and click **Compare**.
Click **Restored database** file that was uploaded as a part of step 13 of this procedure.

b. Verify that the output window matches the database.

> **Note**
>
> - As expected, the user will see a database mismatch with respect to the VMs NodeIDs. Proceed if this is the only difference, if not, contact My Oracle Support (MOS).
> - Archive content and database compatibilities must consist the following:
>   - Archive Contents: Configuration data
>   - Database Compatibility: The databases are compatible.
> - When restoring from an existing backup database to a database using a single NOAM, the expected outcome for the topology compatibility check is as follows:
>   - Topology compatibility: Topology must be compatible minus the NODEID.
> - Attempting to restore a backed-up database onto a NOAM database which is empty. In the context of Topology Compatibility, this text is expected.
> If the verification is successful, click **Back** and continue to next step of this procedure.

10. Restore the database:

a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.

b. Select the **Active NOAM** server and click **Restore**. Select the appropriate backup provisioning and configuration file and click **OK**.

> **Note**
>
> As expected, the user will see a database mismatch with respect to the VMs NodeIDs. Proceed if this is the only difference, if not, contact My Oracle Support (MOS).

c. Select the **Force** checkbox and click **OK** to proceed with the database restore.

> **Note**
>
> After the restore has started, the user will be logged out of **XMI NO GUI** since the restored Topology is old data.

11. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`. Log in as the guiadmin user.

12. Monitor and confirm database restoral. Wait for 5 to10 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:

a. 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.
> - The maintenance and configuration data will be in the same state as when it was first backed up.

13. Log in to the recovered Active NOAM through SSH terminal as admusr user.
14. Re-enable provisioning:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Click **Enable Provisioning** a pop-up window will appear to confirm and click **OK**.
15. Install the second NOAM server by running the following procedure:
    a. Run steps 1 and 3 to 7 Configure the Second NOAM Server.
16. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
    a. Click **Restart** and click **Ok** on the confirmation screen.

> **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.

17. Recover the remaining SOAM servers (standby, spare) by repeating the following steps for each SOAM server:
    a. Install the remaining SOAM servers by running steps 1 and 3 to 7 configure the SOAM Servers.

> **Note**
>
> Before continuing, wait for server to reboot.

18. Restart DSR application:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
    b. Select the recovered server and click **Restart**.
19. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    a. Click **Edit**, for each server whose "Max Allowed HA role" is not Active, set it to **Active** and click **OK**.
20. Restart DSR application:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Server**.
    b. Select each recovered server and click **Restart**.

21. Activate optional features:
    a. Establish an SSH session to the active NOAM, log in as admusr.

> **Note**
>
> - If PCA is installed in the system that is being recovered, perform the following procedures on all the active applications:
>   – PCA Activation on Standby NOAM on recovered Standby NOAM server
>   – PCA Activation on Active SOAM on recovered Active SOAM Server from to re-activate PCA
>
> For more information about the above mentioned procedures, see *Diameter Signaling Router Policy and Charging Application User Guide.*

Refer to Optional Features to activate any features that were previously activated.

> **Note**
>
> - While running the activation script, the following error message (and corresponding messages) output may be seen, the error can be ignored `iload#31000{S/W Fault}`.
> - If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.

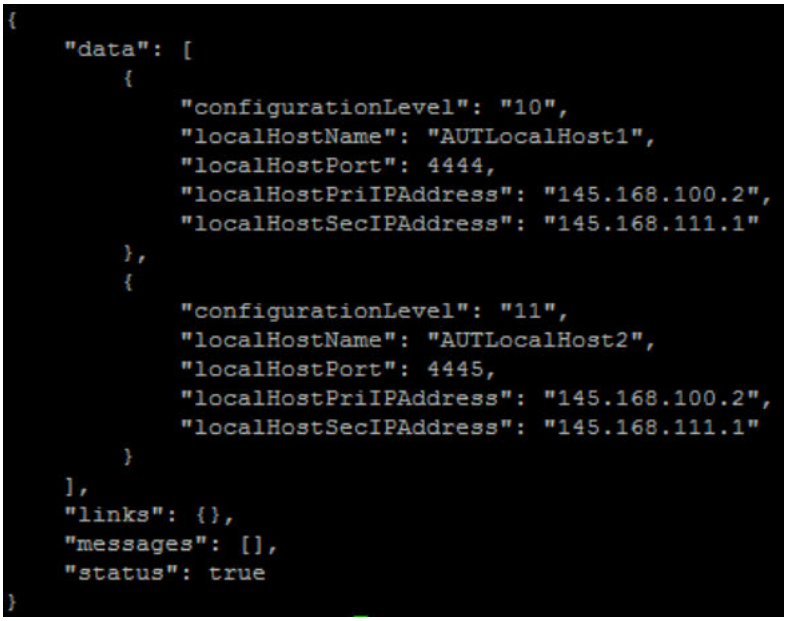
22. Fetch and store the database report for the newly restored data and save it:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Select the Active NOAM server and click **Report**.
    c. Click **Save** and save the report to the local machine.
23. Verify replication between servers:
    a. Log in to the Active NOAM through SSH terminal as admusr user.
    b. Run 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
```

24. Verify the database states:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    b. Verify that the "OAM Max HA Role" is either **Active** or **Standby** for NOAM and SOAM and "Application Max HA Role" for MPs is **Active**, and that the status is **Normal**.
25. Verify the HA Status:
    a. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    b. Select the row for all of the servers, verify that the **HA** role is either **Active** or **Standby**.
26. Verify the local Node Info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Local Node**.
    b. Verify that all the local nodes are shown.
27. Verify the Peer Node Info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Peer Node**.
    b. Verify that all the peer nodes are shown.
28. Verify the Connections Info:
    a. Navigate to **Main Menu**, **Diameter**, **Configuration**, and then **Connections**.
    b. Verify that all the connections are shown.
29. To verify the vSTP MP local nodes info:
    a. Log in to the SOAM VIP Server console as admusr.
    b. Run the following command `[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts`
    c. Verify if the output is similar to the below output.

Figure 4-7 Output

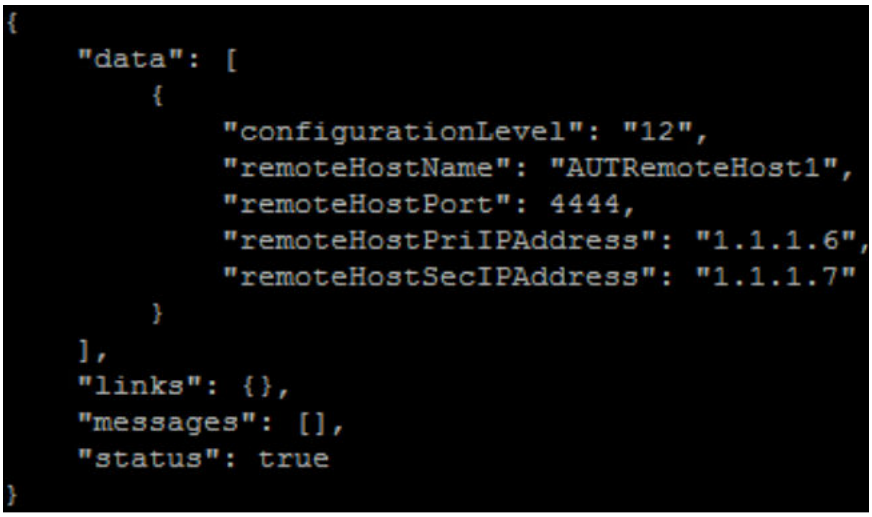


30. To verify the vSTP MP remote nodes info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command:

```
[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
```

    c. Verify if the output is similar to the below output:

Figure 4-8 Output

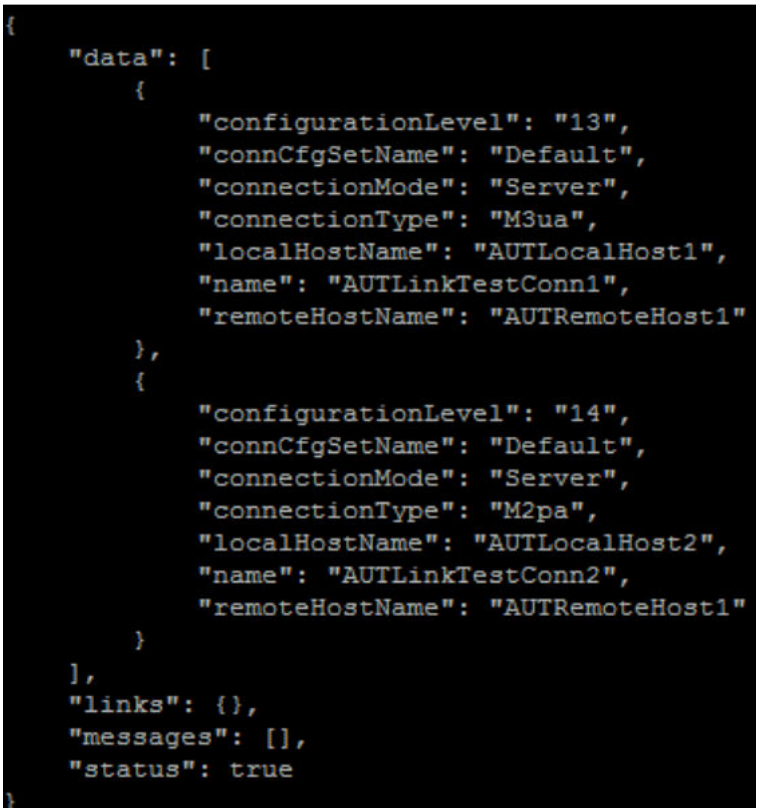


31. To verify the vSTP MP Connections info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command:

```
[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections
```

    c. Verify if the output is similar to the below output:

Figure 4-9 Output



32. Enable Connections if needed:
    a. Navigate to **Main Menu**, **Diameter**, **Maintenance**, and then **Connections**.
    b. Select each connection and click **Enable**. Alternatively you can enable all the connections by selecting **EnableAll**.
    c. Verify that the "Operational State" is **Available**.
33. Enable optional features:
    a. Navigate to **Main Menu**, **Diameter**, **Maintenance**, and then **Applications**.
    b. Select the optional feature application configured before and click **Enable**.
34. If required, re-enable transport:
    a. Navigate to **Main Menu**, **Transport Manager**, **Maintenance**, and then **Transport**.
    b. Select each transport and click **Enable**.
    c. Verify that the operational status for each transport is Up.
35. Re-enable MAPIWF application if needed:
    a. Navigate to **Main Menu**, **Sigtran**, **Maintenance**, and then **Local SCCP Users**.
    b. Click **Enable** corresponding to MAPIWF application Name.
    c. Verify that the SSN status is **Enabled**.
36. Re-enable links if needed.
    a. Navigate to **Main Menu**, **Sigtran**, **Maintenance**, and then **Links**.
    b. Click **Enable** for each link.

c. Verify that the operational status for each link is up.

37. Examine All Alarms:
    a. Navigate to **Main Menu**, **Alarms & Events** and **View Active**.
    b. Examine all active alarms and refer to the on-line help on how to address them. For any queries contact My Oracle Support (MOS).
38. Perform key exchange with Export Server:
    a. Navigate to **Main Menu**, **Administration**, **Remote Servers** and then **Data Export**.
    b. Click **Key Exchange**, enter the password and click **OK**.
39. Examine All Alarms:
    a. Navigate to **Main Menu**, **Alarms & Events** and **View Active**.
    b. Examine all active alarms and refer to the on-line help on how to address them. For any queries contact My Oracle Support (MOS).
40. Restore GUI usernames and passwords:
    a. If applicable, run steps in Section 6.0 to recover the user and group information restored.
41. Backup and archive all the databases from the recovered system:
    a. Run DSR database backup to back up the Configuration databases.

4.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)

For a partial outage with an NOAM server and an SOAM server intact and available, only base recovery of software is needed. The intact NOAM and SOAM servers are capable of restoring the database via replication to all 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 NOAM server by recovering software.

The database is intact at the active NOAM server and does not require restoration at the standby NOAM server.

- Recover any failed SO and MP servers by recovering software.
- Recover the software.

The database in intact at the active NOAM server and does not require restoration at the SOAM and MP servers.

- Re-apply signaling networks configuration if the failed VM is an MP.

Perform the following procedure for recovery if at least 1 NOAM and SOAM server is intact and available:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Refer Workarounds for Issues not fixed in this Release to understand or apply any workarounds required during this procedure.
2. Gather the documents and required materials listed in the Required Materials section.
3. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`. Log in as the guiadmin user.
4. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
   a. Click **Edit** and set "Max Allowed HA Role" to **OOS** and click **OK**.
5. VMware based deployments:
   a. For NOAMs run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure NOAM guests based on resource profile.
   b. For SOAMs run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure Remaining DSR guests based on resource profile
   c. For failed MPs run the following procedures:
      i. Import DSR OVA.

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

      ii. Configure Remaining DSR guests based on resource profile.
   d. For NOAMs run the following procedures:
      i. Import DSR OVA.

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

      ii. Configure NOAM guests based on resource profile.

e. For SOAMs run the following procedures:

i. Import DSR OVA.

> **Note**
>
> If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

ii. Configure Remaining DSR guests based on resource profile.

f. For OVM-S/OVM-M based deployments run the following procedures:

i. Import DSR OVA and prepare for VM creation.

ii. Configure each DSR VM.

> **Note**
>
> While running procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs). For more information, see *Diameter Signaling Router Cloud Installation Guide*.

6. If required, repeat step 5 for all remaining failed servers.
7. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`. Login as the guiadmin user:
8. Install the second NOAM server by running the following procedures:
   a. Configure the Second NOAM Server, steps 1, 3 to 7.
   b. Configuring the NOAM Server Group, step 4

> **Note**
>
> If topology or nodeId alarms are persistent after the database restore, refer to Workarounds for Issues not fixed in this Release or continue with the next step.

9. If the failed server is an SOAM, recover the remaining SOAM servers (standby, spare) by repeating the following steps for each SOAM server:
   a. Install the remaining SOAM servers, configure the SOAM Servers, step 1 and 3 to 7.

> **Note**
>
> Before continuing to next step, wait for the server to restart.

10. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    a. Click **Edit** for each server whose "Max Allowed HA Role" is set to **Standby**, set it to **Active** and click **OK**.
11. Navigate to **Main Menu**, **Status & Manage**, and then **Server**. Select the recovered server and click **Restart**.

12. Establish a SSH session to the C Level server being recovered, log in as admusr.
    a. Run the following procedure for each server that has been recovered.
        i. Configure the MP Virtual Machines, Step 1 and 8 to 14 (step 15 if required).
13. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    a. Click **Edit** for each server whose "Max Allowed HA Role" is set to **Standby**, set it to **Active** and click **OK**.
14. Navigate to **Main Menu**, **Status & Manage**, and then **Server**. Select the recovered servers and click **Restart**.
15. Log in to the recovered Active NOAM through SSH terminal as admusr user.
16. Perform key exchange between the Active NOAM and recovered servers:
    a. Establish an SSH session to the Active NOAM, log in as admusr.
    b. Run the following command to perform a keyexchange from the active NOAM to each recovered server:

```
$ keyexchange admusr@<Recovered Server Hostname>
```

17. Activate optional features:
    a. Establish an SSH session to the active NOAM, log in as admusr.

> **Note**
>
> - If PCA is installed in the system that is being recovered, perform the following procedures on all the active applications:
>   – PCA Activation on Standby NOAM on recovered Standby NOAM server
>   – PCA Activation on Active SOAM on recovered Active SOAM Server from to re-activate PCA
>
> For more information about the above mentioned procedures, see *Diameter Signaling Router Policy and Charging Application User Guide.*

    b. Refer to Optional Features to activate any features that were previously activated.

> **Note**
>
> - While running the activation script, the following error message (and corresponding messages) output may be seen, which can be ignored `iload#31000{S/W Fault}`.
> - If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.

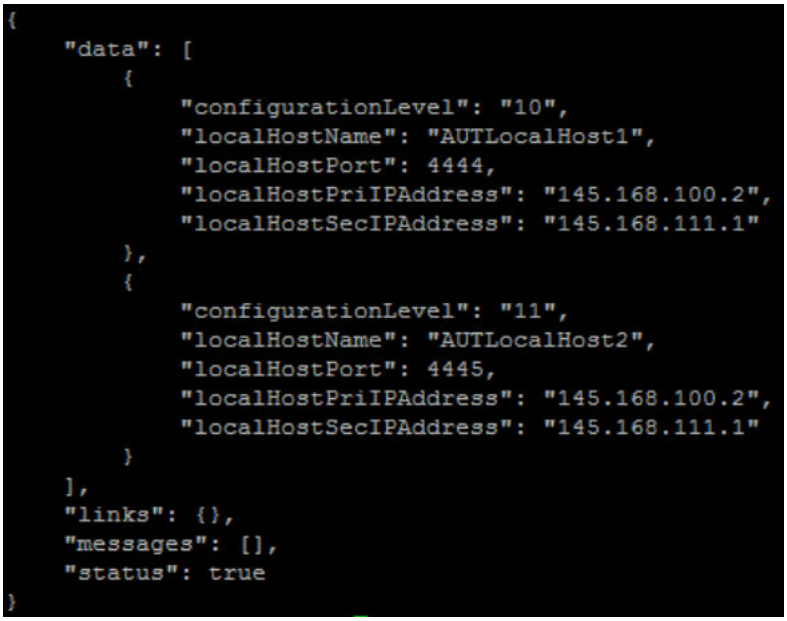
18. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    a. Select the Active NOAM server and click **Report**.
    b. Click **Save** to save the report to the local machine.

19. Log in to the Active NOAM through SSH terminal as admusr user. Run 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
```

20. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
    a. Verify that the "OAM Max HA Role" is either "Active" or "Standby" for NOAM and SOAM and "Application Max HA Role" for MPs is **Active**, and the status is **Normal**.
21. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
    a. Select the row for all the servers. Verify that the **HA Role** is either **Active** or **Standby**.
22. Navigate to **Main Menu**, **Diameter**, **Configuration** and then **Local Node**. Verify that all the peer nodes are shown.
23. Navigate to **Main Menu**, **Diameter**, **Configuration** and then **Connections**. Verify that all the connections are shown.
24. To verify the vSTP MP local nodes info:
    a. Log in to the SOAM VIP Server console as admusr.
    b. Run the following command `[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts`
    c. Verify if the output is similar to the below output.

Figure 4-10 Output



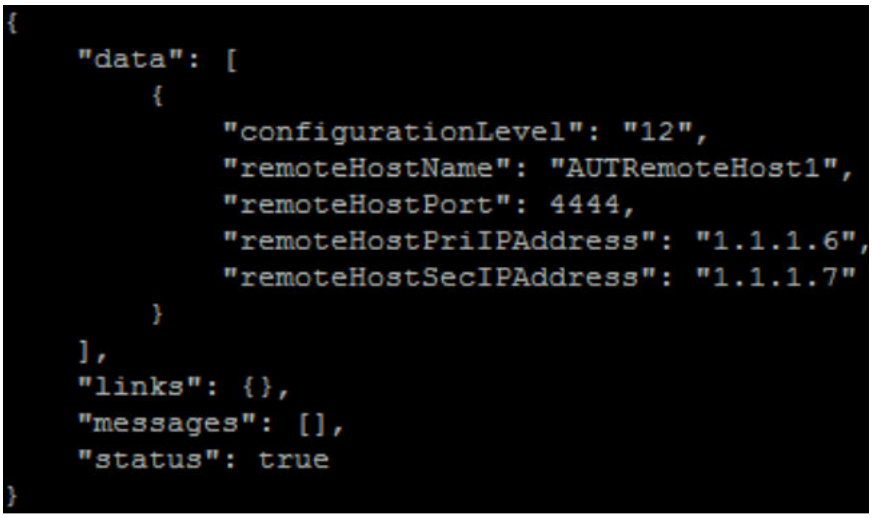
```
{
    "data": [
        {
            "configurationLevel": "10",
            "localHostName": "AUTLocalHost1",
            "localHostPort": 4444,
            "localHostPriIPAddress": "145.168.100.2",
            "localHostSecIPAddress": "145.168.111.1"
        },
        {
            "configurationLevel": "11",
            "localHostName": "AUTLocalHost2",
            "localHostPort": 4445,
            "localHostPriIPAddress": "145.168.100.2",
            "localHostSecIPAddress": "145.168.111.1"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```


25. To verify the vSTP MP Remote nodes info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command:

    ```
    [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
    ```

    c. Verify if the output is similar to the below output:

Figure 4-11 Output



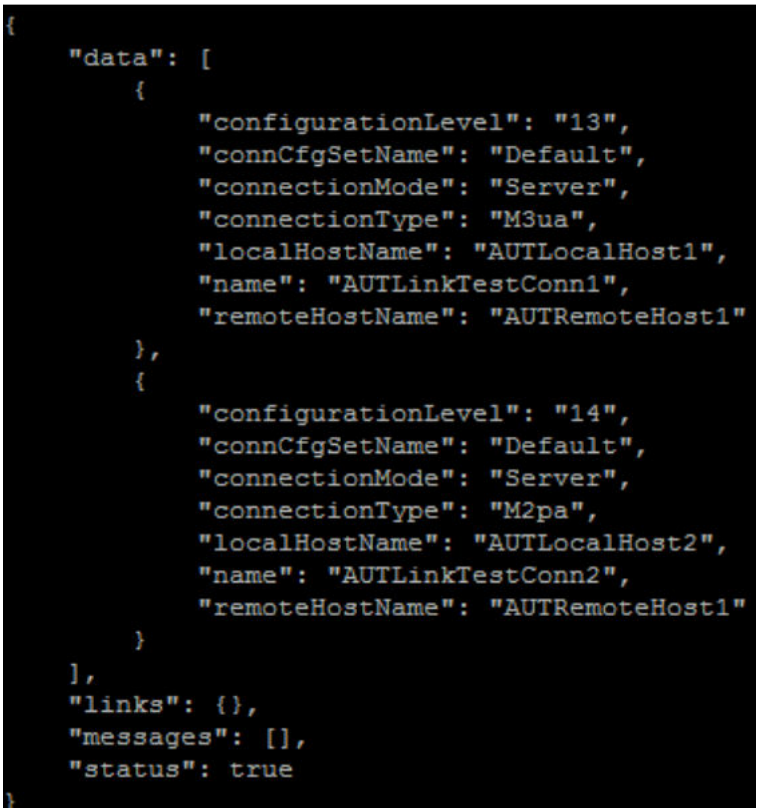
```
{
    "data": [
        {
            "configurationLevel": "12",
            "remoteHostName": "AUTRemoteHost1",
            "remoteHostPort": 4444,
            "remoteHostPriIPAddress": "1.1.1.6",
            "remoteHostSecIPAddress": "1.1.1.7"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```


26. To verify the vSTP MP Connections info:
    a. Log in to the SOAM VIP server console as admusr.
    b. Run the following command:

    ```
    [admusr@SOAM1 ~]$ mmiclient.py /vstp/connections
    ```

c. Verify if the output is similar to the below output:

Figure 4-12 Output



27. Disable SCTP Auth Flag:
    a. For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix.
    b. Run this procedure on all failed MP servers.
28. Navigate to **Main Menu**, **Diameter**, and then **Connections**.
    a. Select each connection and click **Enable**.
    b. Alternatively enable all the connections by selecting **EnableAll**.
    c. Verify that the operational state is **Available**.
29. Navigate to **Main Menu**, **Diameter**, **Maintenance** and then **Applications**.
    a. Select the optional feature application and click **Enable**.
30. Navigate to **Main Menu**, **Transport Manager**, **Maintenance** and then **Transport**.
    a. Select each transport and click **Enable**.
    b. Verify that the operational status for each transport is Up.
31. Navigate to **Main Menu**, **Sigtran**, **Maintenance** and then **Local SCCP Users**.
    a. Click **Enable** corresponding to MAPIWF application name.
    b. Verify that the SSN Status is **Enabled**.
32. Navigate to **Main Menu**, **Sigtran**, **Maintenance** and then **Links**.

a. Click **Enable** for each link.

b. Verify that the operational status for each link is up.

33. Examine All Alarms:

a. Navigate to **Main Menu**, **Alarms & Events**, and then **View Active**.

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

ii. If required contact My Oracle Support (MOS).

34. If required, restart `oampAgent`.

> **Note**
>
> If alarm 10012 the responder for a monitored table failed to respond to a table change is raised, the `oampAgent` needs to be restarted.

a. Establish an SSH session to each server that has the alarm. Log in as admusr.

b. Run the following commands:

```
$ sudo pm.set off oampAgent
$ sudo pm.set on oampAgent
```

35. Run DSR database backup to backup the configuration databases.

4.1.5 Recovery Scenario 5 (Partial server outage with both NOAM servers failed with DR-NOAM Available)

For a partial outage with both NOAM servers failed but a DR NOAM available, the DR NOAM is switched from secondary to primary then recovers the failed NOAM 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 run the procedure. The major activities are summarized as follows:

Switch DR NOAM from secondary to primary

Recover the failed NOAM servers by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- The database is intact at the newly active NOAM server and does not require restoration.

If applicable, recover any failed SOAM and MP servers by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- The database in intact at the Active NOAM server and does not require restoration at the SOAM and MP servers.

Perform the following procedure for recovery if both NOAM servers have failed but a DR NOAM is available:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Refer Workarounds for Issues not fixed in this Release to understand or apply any workarounds required during this procedure.
2. Gather the documents and required materials listed in the Required Materials section.
3. Refer *Diameter Signaling Router SDS NOAM Failover User Guide*.
4. For VMWare based deployments:
   a. For NOAMs run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure NOAM guests based on resource profile.
   b. For SOAMs run the following procedures:
      i. Import DSR OVA

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

      ii. Configure Remaining DSR guests based on resource profile
   c. For failed MPs run the following procedures:
      i. Import DSR OVA.

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

      ii. Configure remaining DSR guests based on resource profile.

      For KVM or Openstack based deployments:
   d. For NOAMs run the following procedures:
      i. Import DSR OVA.

      > **Note**
      >
      > If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA

ii. Configure NOAM guests based on resource profile.

e. For SOAMs run the following procedures:

i. Import DSR OVA.

> **Note**
>
> If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA.

ii. Configure Remaining DSR guests based on resource profile.

f. For OVM-S/OVM-M based deployments run the following procedures:

i. Import DSR OVA and prepare for VM creation.

ii. Configure each DSR VM.

> **Note**
>
> Configure the required failed VMs only (NOAMs/SOAMs/MPs).

5. If all SOAM servers have failed, run Partial Server Outage with One NOAM Server Intact and both SOAMs Failed.
6. Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM server. Open the web browser and enter the following url `http://<Primary_DR-NOAM_VIP_IP_Address>`. Log in as the guiadmin user.
7. Navigate to **Main Menu**, click **Status & Manage**, and then **HA**.
   a. Click **Edit**, select the standby for the failed NOAM servers and click **OK**.
8. Navigate to **Main Menu**, **Configuration**, and then **Servers**.
   From the GUI screen, select the failed NOAM server and then select **Export** to generate the initial configuration data for that server
9. Obtain a terminal session to the DR-NOAM VIP, log in as the admusr user. Run the following command to configure the failed NOAM server:

```
$ sudo scp -r
/var/TKLC/db/filemgmt/TKLCConfigData.<Failed_NOAM_Hostnam
e>.sh
admusr@<Failed_NOAM_xmi_IP_address>:/var/tmp/TKLCConfigDa
ta.sh
```

10. Establish an SSH session to the recovered NOAM server (Recovered_NOAM_xmi_IP_address).
    a. Log in as the admusr user.
    The automatic configuration daemon will look for the file named "TKLCConfigData.sh" in the `/var/tmp` directory, implement the configuration in the file, and then prompt the user to reboot the server.

b. Verify `awpushcfg` called by checking the following file

```
$ sudo cat /var/TKLC/appw/logs/Process/install.log
Verify the following message is displayed:
[SUCCESS] script completed successfully!
```

c. Following is the command to reboot the server:

```
$ sudo init 6
```

Wait for the server to restart.

11. Run the following command on the failed NOAM server and ensure that no errors are returned:

```
$ sudo syscheck
Running modules in class hardware...OK
Running modules in class disk...OK
Running modules in class net...OK
Running modules in class system...OK
Running modules in class proc...OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

12. Repeat steps 8 to 11 for the 2nd failed NOAM server.

13. Perform a keyexchange between the newly active NOAM and the recovered NOAM servers:
From a terminal window connection on the active NOAM as the admusr user, exchange SSH keys for admusr between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs.

When prompted for the password, enter the password for the admusr user of the recovered NOAM servers.

```
$ keyexchange admusr@<Recovered_NOAM Hostname>
```

14. Navigate to **Main Menu**, **Configuration**, and then **HA**

a. Click Edit, for each NOAM server whose "Max Allowed HA" role is set to **Standby**, set it to **Active** and click **OK**.

15. Navigate to **Main Menu**, click **Status & Manage**, and then **Server**.
Select each recovered NOAM server and click **Restart**.

16. Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows:

a. For PCA: Establish SSH sessions to all the recovered NOAM servers and log in as admusr. Refer and run procedure "PCA Activation on Standby NOAM" server on all recovered NOAM Servers to re-activate PCA.

i. Establish SSH session to the recovered active NOAM, login as admusr. Refer activate Map-Diameter Interworking (MAP-IWF).

> **Note**
>
> - While running the activation script, the following error message (and corresponding messages) output may be seen which can be ignored `iload#31000{S/W Fault}`.
> - If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.

17. Switch DR NOAM back to secondary: After the system has been recovered. Refer to Diameter Signaling router SDS NOAM Failover Users Guide.
18. Navigate to **Main Menu**, **Administration**, **Remote Servers** and then **Data Export**.
    a. Click **Key Exchange**. Enter the password and click **OK**.
19. Navigate to **Main Menu**, **Alarms & Events**, and then **View Active**.
20. Verify the recovered servers that are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc).
21. If required, refer Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact) recover any standby or spare SOAMs as well as any C-Level servers.

4.1.6 Recovery Scenario 6 (Database Recovery)

Case 1

For a partial outage with Cloud Disaster Recovery guide:

- Server having a corrupted database.
- Replication channel from parent is inhibited because of upgrade activity.
- Due to upgrade activities, the server is in a different release than its active parent.
- Verify that the Server runtime backup files performed at the start of the upgrade are present in `/var/TKLC/db/filemgmt` area in the following format:
  - Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
  - Backup.DSR.HPC02-NO2.FullRunEnv.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

> **Note**
>
> During recovery, the corrupted database will get replaced by the sever runtime backup. Any configuration done after taking the backup will not be visible post recovery.

Perform the following procedure for recovery if database is corrupted in the system:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.

1. Refer Workarounds for Issues not fixed in this Release to understand or apply any workarounds required during this procedure.
2. Navigate to **Main Menu**, **Status & Manage**, and then **HA**.
3. Select **Edit** and from the dropdown menu, set the "Max Allowed HA" role to **OOS** for the failed servers and Select **OK**.
4. Establish an SSH session to the server in question. Log in as an admusr user.
5. Run the following command to bring the system to runlevel 3:

   ```
   $ sudo init 3
   ```

6. Run the following command and follow the instructions appearing in the console prompt:

   ```
   $ sudo /usr/TKLC/appworks/sbin/backout_restore
   ```

7. Run the following command to bring the system back to runlevel 4:

   ```
   $ sudo init 6
   ```

8. Run the following command to verify if the processes are up and running:

   ```
   $ sudo pm.getprocs
   ```

9. Navigate to **Main Menu**, and then **Status & Manage**, and then **HA**.
10. Click Edit, for each failed server whose Max Allowed HA Role is set to OOS, set it to **Active** and click **OK**.
11. Run DSR database backup to back up the Configuration databases.

Case 2

For a partial outage with:

- Server having a corrupted database.
- Replication channel is not inhibited.
- Server has the same release as that of its Active parent.

Perform the following procedure if database got corrupted in the system and system is in the state to get replicated:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Refer to any workarounds required during this procedure.
2. Navigate to **Main Menu**, and then **Status & Manage**, and then **HA**.
3. Click **Edit** and from the dropdown menu, set the "Max Allowed HA" role to **OOS** for the failed servers and select **OK**.
4. Establish an SSH session to the server in question. Log in as admusr user.

5. Run the following command to take the server out of service.

```
$ sudo bash –l
$ sudo prod.clobber
```

6. Run the following commands to take the server to `Dbup` and start the DSR application:

```
$ sudo bash –l
$ sudo prod.start
```

   a. Run the following command to verify if replication channels are up and running:

      ```
      $ sudo irepstat
      ```

   b. Run the following command to verify if merging channels are up and running:

      ```
      $ sudo inetmstat
      ```

7. Navigate to **Main Menu**, and then **Status & Manage**, and then **Server**. Select each recovered server and click **Restart**.
8. Navigate to **Main Menu**, and then **Status & Manage**, and then **HA**.
   a. Click **Edit** and from the dropdown menu, set the "Max Allowed HA" role to **OOS** for the failed servers and select **OK**.
9. Run DSR database backup to back up the Configuration databases.

5 Resolving User Credential Issues after Database Restore

User incompatibilities may introduce security holes or prevent access to the network by administrators. Inconsistencies among users are not considered a threat to the database, however. Review each user difference carefully to ensure that the restoration will not impact security or accessibility.

5.1 Restoring a Deleted User

These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

Figure 5-1 Testuser

```
- User 'testuser' exists in the selected backup file but not in the current
database.
```

5.2 Keeping a Restored user

Perform the following procedure to keep users that will be restored by system restoration:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`.
2. Navigate to **Administration**, **Access Control**, and then **Users**.
   a. Select the user and click **Change Password**.
   b. Enter a new password and click **Continue**.

5.3 Removing a Restored User

Perform the following procedure to remove users that will be restored by system restoration:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`.
2. After restoration delete user:
   a. Navigate to Administration, Access Control, and then Users.
   b. Select the user and click **Delete**.
   c. Click **Ok** to confirm.

5.4 Restoring a Modified User

Before the backup and archive files were created, the passwords for these users are changed.

Figure 5-2 Test user

```
- The password for user 'testuser' differs between the selected backup file
and the current database.
```

Before Restoration:

Verify access to an user with administrator permissions. Contact every impacted user and let them know that their password will be changed while this maintenance is being done.

After Restoration:

All users in this category should log in and have their passwords reset. To reset a user's password, follow the instructions in My Oracle Support (MOS).

5.5 Restoring an Archive that does not contain a Current User

These users have been created after the creation of the backup and archive file. The user will be deleted by system restoration of that file.

Figure 5-3 Test user

```
- User 'testuser' exists in current database but not in the selected backup
file.
```

If the user no longer exist, do not perform any additional steps. The user is permanently removed.

Perform the following procedure to remove users that will be restored by system restoration:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Notify affected users before restoration:
   a. Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2. Log in to the NOAM VIP:
   a. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://Primary_NOAM_VIP_IP_Address>`.
3. Navigate to **Administration**, **Access Control**, and then **Users**. Under each affected user, record the following:
   a. Username
   b. Account status
   c. Remote Auth
   d. Local Auth
   e. Concurrent Logins Allowed
   f. Inactivity Limit
   g. Comment
   h. Groups
4. After restoration:
   a. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter the following url `http://<Primary_NOAM_VIP_IP_Address>`.
5. After Restoration recreate affected user and required group:
   a. Navigate to **Administration**, **Access control**, and then **Users**.
   b. Click **Insert** and recreate the user using the data collected in step 4 and click **OK**.
6. Repeat step 5 to recreate additional users and groups.
7. After restoration reset the passwords.

6
IDIH Disaster Recovery

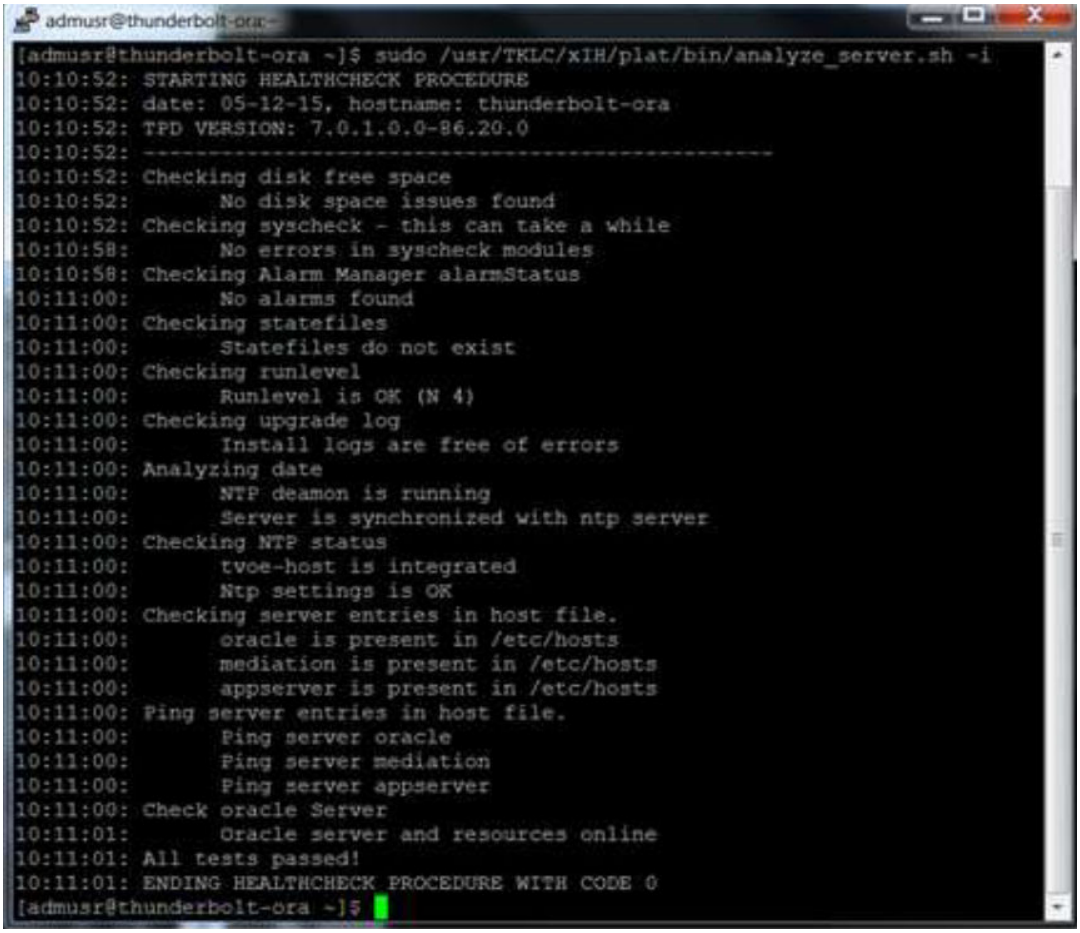
Following are the procedures for disaster recovery preparation steps for the IDIH:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Establish an SSH session to the Oracle guest, log in as admusr.
2. Run the following command to perform a database health check:

```
$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i
```

Figure 6-1 Output



> **Note**
>
> If this step fails, a reinstallation is required.

For VMware based deployments:

a. Create iDIH Virtual Machines (VMWare)

b. Configure iDIH Virtual Machines

For KVM/Openstack based deployments:

a. Create iDIH Virtual Machines (KVM/Openstack)

b. Configure iDIH Virtual Machines

For OVM-S/OVM-M based deployments:

a. (OVM-S/OVM-M). Import three IDIH OVA's and create and configure a VM for each.

b. Configure iDIH Virtual Machines

For OL7 and KVM based deployments:

a. Installation on OL7 and KVM

b. Post iDIH Installation Configuration

IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Perform the following procedure to recover the application and mediation VMs:
   For VMWare based deployments:

   Create iDIH Oracle, Mediation and Application VMs.

   For KVM / Openstack based deployments:

   Create iDIH Oracle, Mediation and Application VMs (Optional).

   For OVM-S / OVM-M based deployments:

   Import three IDIH OVA's and create and configure a VM for each.
2. Configure iDIH VM Networks:
   a. Run the following procedure from [1] to configure the VM networks on the Application and Mediation VMs only.
      Configure iDIH VM Networks
3. Configure VMs:
   a. Run post installation scripts on iDIH VMs, step 3 to 7.
4. If integration is needed run the following procedure:
   a. Integrate iDIH into DSR

A.1 DSR Database Backup

Perform the following procedure to back up the provision and configuration information from NOAM or SOAM server after the disaster recovery is complete:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server.
   a. Open the web browser and enter the following url `http://<Primary_NOAM/SOAM_VIP_IP_Address>`.
2. Backup configuration on data for the System:
   a. Navigate to **Main Menu**, **Status & Manage**, and then **Database**.
   b. Select the Active NOAM Server and click **Backup**.
   c. Check the checkbox next to configuration.
   d. Enter the filename for the backup and click **OK**.
3. Navigate to **Main Menu**, **Status & Manage**, and then **Files**.
   a. Select the Active NOAM or SOAM tab. The files on this server will be displayed. Verify the existence of the backup file.
4. Download the file to a local machine.
   a. From the previous step, choose the backup file and select **Download**.
   b. Select **OK** to confirm the download.
5. Upload the Image to Secure Location:
   a. 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. Repeat steps 2 through 5 to back up the Active SOAM.

A.2 Un-Inhibit A and B Level Replication on C-Level Servers

Perform the following procedure to Un-inhibit A and B level replication on all C Level servers:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

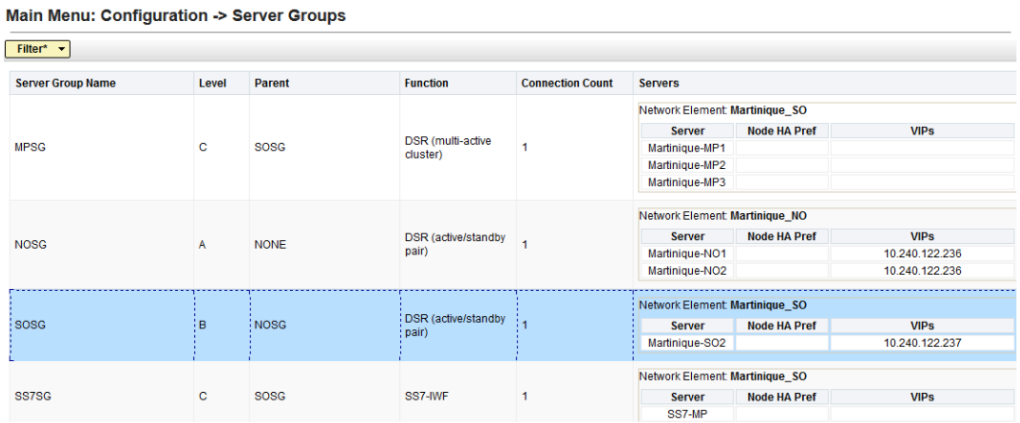
1. Log in to the Active NOAM server through SSH as admusr user.
2. Un-Inhibit replication on all C level Servers:
   a. Run the following command:

```
$ for i in $(iqt -p -z -h -fhostName NodeInfo where
"nodeId like 'C*' and siteId='<NE name of the site>'");
do iset -finhibitRepPlans='' NodeInfo where
"nodeName='$i'"; done
```

> **Note**
>
> To find the site's NE name, go to Active NOAM GUI and navigate to **Configuration** and **Server Groups** tab.

For more information, refer the below screenshot:

Figure 2 Group-server



3. After running above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
   Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site example: Site SO_HPC03 shall be set as empty.

Perform the following command:

```
$ sudo iqt NodeInfo
Expected output:
nodeId     nodeName hostName nodeCapability inhibitRepPlans siteId
excludeTables
A1386.099     NO1     NO1     Active                         NO_HPC03
B1754.109     SO1     SO1     Active                         SO_HPC03
C2254.131     MP2     MP2     Active                         SO_HPC03
C2254.233     MP1     MP1     Active                         SO_HPC03
```

A.3 Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

Perform the following procedure to inhibit A and B level replication on all C level servers of this site (when Active, Standby and Spare SOAMS are lost):

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Log in to the Active NOAM server through SSH as admusr user.
2. Inhibit replication on all C level Servers:
   a. Run the script (if available) from:

```
/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh


/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh --replication=inhibit
-- SO_SG_Name=<SOAM server group name>
```

   If script doesn't exist run the below command manually (if above mentioned script is not present in the specific path):

Figure 3 SOAM server group name

```
$ for i in $(sudo Imysql.client -B -N -e "
SELECT DISTINCT CS.hostname
  FROM appworks.Server CS, appworks.Server PS,
appworks.Server2SG C2SG, appworks.Server2SG P2SG,
appworks.ServerGroup CSG, appworks.ServerGroup PSG,
comcol.ClusterInfo CCI, comcol.ClusterInfo PCI,
comcol.ClusterGroupInfo
  WHERE CS._h_Server_ID = C2SG._h_Server_ID
    AND C2SG._h_SG_ID = CSG._h_SG_ID
    AND CSG.clusterId = CCI.clusterId
    AND CCI.groups = comcol.ClusterGroupInfo.groupId
    AND comcol.ClusterGroupInfo.parentGroup = PCI.groups
    AND PCI.clusterId = PSG.clusterId
    AND PSG.ServerGroupName='<SOAM_SG_NAME>'
"); do iset -finhibitRepPlans='A B' NodeInfo where
"nodeName='$i'"; done
```

> **Note**
>
> To find the site's SOAM_SG_NAME, go to Active NOAM GUI and navigate to **Configuration** and **Server Groups** tab.

For more information refer to the following screenshot:

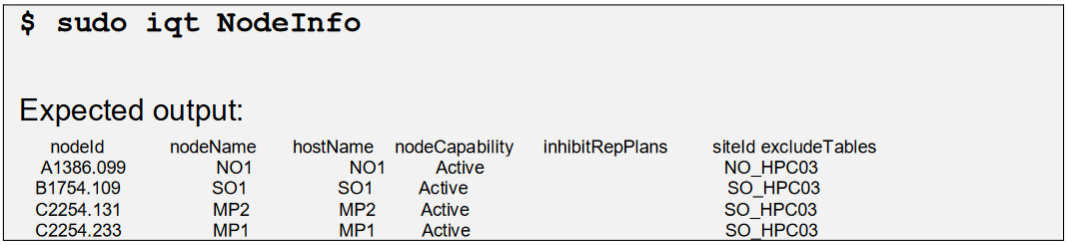
Figure 4 Server groups

No warnings would appear on the GUI indicating that replication on MP is disabled after completing the previously stated procedures to un-inhibit replication on MP(s).

Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group example: Server group SO_SG shall be set as ‘ ’:

3. Perform the following command manually:

Figure 5 Nodeinfo



A.4 Inhibit A and B Level Replication on C-Level Servers

Perform the following procedure to inhibit A and B level replication on all C Level servers:

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Log in to the Active NOAM server through SSH as admusr user.
2. Run the following command manually:

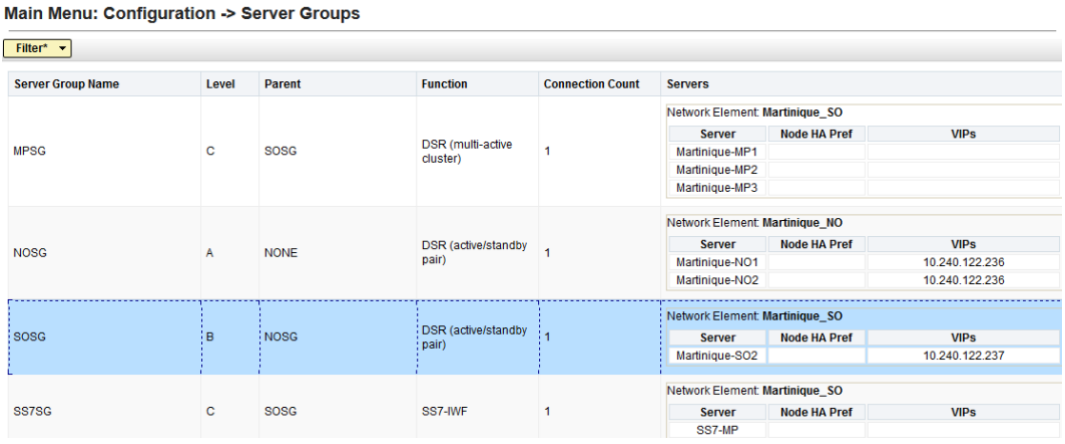
Figure 6 Command

```
$ for i in $(iqt -p -z -h -fhostName NodeInfo where
"nodeId like 'C*' and siteId='<NE name of the site>'");
do iset -finhibitRepPlans='A B' NodeInfo where
"nodeName='$i'"; done
```

> **Note**
>
> To find the site's NE name, go into the Active NOAM GUI and navigate to **Configuration** and **Server Groups** tab.

For more information, see the screenshot below:

Figure 7 Server groups



3. After running above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.

Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site example: Site SO_HPC03 shall be set as empty.

Perform the following command manually:

Figure 8 Command

```
$ sudo iqt NodeInfo
```

Expected output:

nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId	excludeTables
A1386.099	NO1	NO1	Active		NO_HPC03	
B1754.109	SO1	SO1	Active		SO_HPC03	
C2254.131	MP2	MP2	Active	A B	SO_HPC03	
C2254.233	MP1	MP1	Active	A B	SO_HPC03	

A.5 Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

Perform the following procedure to un-inhibit A and B level replication on all C level servers of this site (when Active, Standby and Spare SOAMS are lost).

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Log in to the Active NOAM server through SSH as admusr user.
2. Run the script from the following command:

```
/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh
```

```
/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh --replication=allow --
SO_SG_Name=<SOAM server group name>
```

3. If the script doesn't exist run the below command manually (alternate to above script (if above mentioned script is not present in the specific path):

Figure 9 Script

```
$ for i in $(sudo Imysql.client -B -N -e "
SELECT DISTINCT CS.hostname
  FROM appworks.Server CS, appworks.Server PS,
appworks.Server2SG C2SG, appworks.Server2SG P2SG,
appworks.ServerGroup CSG, appworks.ServerGroup PSG,
comcol.ClusterInfo CCI, comcol.ClusterInfo PCI,
comcol.ClusterGroupInfo
  WHERE CS._h_Server_ID = C2SG._h_Server_ID
    AND C2SG._h_SG_ID = CSG._h_SG_ID
    AND CSG.clusterId = CCI.clusterId
    AND CCI.groups = comcol.ClusterGroupInfo.groupId
    AND comcol.ClusterGroupInfo.parentGroup = PCI.groups
    AND PCI.clusterId = PSG.clusterId
    AND PSG.ServerGroupName='<SOAM_SG_NAME>'
"); do iset -finhibitRepPlans='' NodeInfo where
"nodeName='$i'"; done
```

> **Note**
>
> To find the site's SOAM_SG_NAME, go to Active NOAM GUI and navigate to **Configuration** and **Server Groups** tab.

For more information refer to the following screenshot:

Figure 10 Server groups

No warnings would appear on the GUI indicating that replication on MP is disabled after completing the previously stated procedures to un-inhibit replication on MP(s).

Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group example: Server group SO_SG shall be set as ‘ ’:

Perform the following command manually:

Figure 11 Nodeinfo

```
$ sudo iqt NodeInfo
```

Expected output:

nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId excludeTables
A1386.099	NO1	NO1	Active		NO_HPC03
B1754.109	SO1	SO1	Active		SO_HPC03
C2254.131	MP2	MP2	Active		SO_HPC03
C2254.233	MP1	MP1	Active		SO_HPC03

4. Verify replication that has been un-Inhibited.

A.6 Workarounds for Issues not fixed in this Release

Perform the following procedure to check and create backup directory.

> **Note**
>
> If this procedure fails, contact My Oracle Support (MOS).

1. Determine if backup directory is created:
   a. Run the following command on console of Active NOAM/SOAM server (accessed via the VIP) and compare the output:

      ```
      $ cd /var/TKLC/db/filemgmt/
      ```

      ```
      $ ls -ltr
      ```

   b. Look for backup directory in the output.
   c. Check if directory is already created with correct permission and directory will look like:

      ```
      drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup
      ```

   d. In case, directory is already there with right permissions then skip step 2 and 3.
   e. If directory is not with right permissions then run step 3 otherwise go to next step.
2. NOAM/SOAM VIP console change permissions of backup directory:
   a. Assuming present working directory exists in `/var/TKLC/db/filemgmt/` if not run

      ```
      cd /var/TKLC/db/filemgmt/
      ```

   b. Create backup directory using the following command:

      ```
      $mkdir backup
      ```

   c. Verify if directory is created:

      ```
      $ ls -ltr /var/TKLC/db/filemgmt/backup
      ```

      Error should not appear, "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content.
3. Assuming present working directory is /var/TKLC/db/filemgmt/ Otherwise run:

   ```
   cd /var/TKLC/db/filemgmt/
   ```

a. Create backup directory:

```
# $mkdir backup
```

b. Verify if directory is created

```
$ ls -ltr/var/TKLC/db/filemgmt/backup
```

Error should not appear, "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content.

4. Assuming backup directory is created.
   a. Verify directory is created:

```
$ ls -ltr/var/TKLC/db/filemgmt/backup
```

Error should not appear, "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content.

   b. If directory is not created proceed to step 2.
   c. Change permissions of backup directory running the following command:

```
$ chmod 770 /var/TKLC/db/filemgmt/backup
```

   d. 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.
```

   e. Directory will look like:

```
drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15 backup
```

5. Copy the backup file to backup directory:

```
$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup.
```

   a. Provide permissions to backup file inside backup directory.
   b. Ensure present working directory `$cd /var/TKLC/db/filemgmt/backup`.
   c. Change permissions of files inside backup directory `$chmod 666`.
   d. Change ownership of files inside backup directory.

```
$ sudo chown -R awadmin:awadm Backup.*
```