Oracle® Communications

DSR BareMetal to Cloud Migration Guide

Release 9.0.1.0.0
F88023-01
October 2023

Oracle Communications DSR BareMetal to Cloud Migration Guide, Release 9.0.1.0.0

F88023-01

Copyright © 2023, Oracle and/or its affiliates.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

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

Contents

My Oracle Support

My Oracle Support

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

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

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

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

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

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

Emergency Response

In the event of a critical service situation, the users can avail emergency response by calling the CAS main number at 1-800-223-1711 (toll-free in the US), or the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center

Oracle Communications' customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these

documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click Industries.
3. Under the Oracle Communications subhead, click the Oracle Communications documentation link. The Communications Documentation page appears. You can see most products covered by these documentation sets under the headings Network Session Delivery and Control Infrastructure or “Platforms.”
4. Click your Product and then the Release Number. A list of the entire documentation set for the selected product and release appears. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser) and save to a local folder.

Acronyms

An alphabetized list of acronyms used in the document is listed below:

Table Acronyms and Terminology

Acronym	Description
BM	BareMetal
CD-ROM	Compact Disc Read-only Media
CPA	Charging Proxy Agent
CSV	Comma-separated Values
DA	Diameter Agent
DAMP	Diameter Agent Message Processor
DB	Database
DCA	Diameter Custom Application
DIU	Dual Image Upgrade
DP	Data Processor
DR	Disaster Recovery
DSR	Diameter Signaling Router
DR NOAM	Disaster Recovery DSR NOAM
EIR	Equipment Identity Register
FABR	Full Address Based Resolution
FOA	First Office Application
GA	General Availability
GPS	Global Product Solutions
GUI	Graphical User Interface
HA	High Availability
IDIH	Integrated Diameter Intelligence Hub
IMI	Internal Management Interface
IP	Internet Protocol
IPM	Initial Product Manufacture
IPFE	IP Front End
ISO	ISO 9660 File System (when used in the context of this document)
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
MW	Maintenance Window
NE	Network Element
NOAM	Network OAM
OAM	Operations, Administration, and Maintenance
OFCS	Offline Charging Solution
PCA	Policy and Charging Agent (formerly known as PDRA)
PDRA	Policy Diameter Routing Agent
RBAR	Range Based Address Resolution
SBR	Session Binding Repository

Table (Cont.) Acronyms and Terminology

Acronym	Description
SDS	Subscriber Database Server
SOAM	System OAM
VIP	Virtual IP
VM	Virtual Machine
XMI	XML Metadata Interchange

1
Introduction

This document provides detailed information to migrate DSR from BareMetal (BM) to Virtual Machine (VM). This document outlines different methods to migrate DSR.

1.1 References

Following are the reference documents:

- *Oracle Communications DSR Cloud Upgrade Document*
- *Oracle Communication DSR Cloud Installation Guide*

2
Overview

Oracle Communications Diameter Signaling Router (DSR) creates a centralized core diameter signaling layer that relieves LTE, IMS, and 3G diameter endpoints of routing, traffic management, and load balancing tasks. DSR provides a single interconnect point to other networks.

This section provides information about DSR Migration from release 8.6.x BareMetal (BM) to 9.0.1 VM and later.

You can migrate DSR from release 8.6.x BM to 9.0.1 VM and later using following methods:

- Method 1: By reusing the existing hardware and IP addresses of NOAM, SOAM, IPFE, and DAMP. Using this method, you can shut down the DSR 8.6.x applications on BM and deploy them on VM using existing IP addresses.
- Method 2: By reusing the existing hardware and new IP addresses of NOAM, SOAM, IPFE, and DAMP. Using this method, you can shut down the DSR 8.6.x applications on BM and deploy them on VM using new IP addresses.
- Method 3: By using new hardware and the existing IP addresses of NOAM, SOAM, IPFE, and DAMP. Using this method, you can shut down the DSR 8.6.x applications on BM and deploy new NOAM, SOAM, IPFE, and DAMP, on VM using existing IP addresses.

> **Note:**
>
> From DSR 9.0.1 and later, there is no support for the BM environment. Therefore, to upgrade from DSR 8.6.x to DSR 9.0.1, you must perform the migration process outlined in this document.

2.1 Prerequisites

You must perform the following tasks to set up the migration environment:

- Verify if the mated site has the capacity to handle the traffic. For information, contact My Oracle Support.
- Run the following command on the Host hardware to check the IP connectivity between BM and VM host hardware.

  ```
  ping (baremetal DSR NOAM IP)
  ```

- Divert all the traffic to the mated site.
- Take a backup of all the servers from the DSR GUI as described in *Full Backup of DB Run Environment at Each Server* in *DSR Cloud Software Upgrade Guide*.
- Export DSR 8.6.x configuration data from NOAM and SOAM as described in Exporting Configuration Data on DSR 8.6.X.

- Run the following commands on Active and Standby NOAM and SOAM one after another:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

- Run the following commands on all C level servers one after another:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

> **Note:**
>
> Store the backed up data on a remote server. This data is required while performing backout.

The following table provides the time requirement by each task while performing migration from BareMetal DSR 8.6.X to DSR 9.0.x VM.

Table 2-1 Time Required for DSR Migration

Procedure	Time Required in minutes
Step 1 - Preparing check list and verifying it	20
Step 2 - Prerequisite checking and procedures	140 **Note:** Provided assuming 2 DR NOAM, 2 NOAM, 2 SOAM
Step 3 - Standby DR NOAM Migration	86
Step 4 - Active DR NOAM Migration	80
Step 5 - Standby NOAM Migration	80
Active NOAM Migration	80
Standby SOAM Migration	80
Active SOAM Migration	80
Standby IPFE Migration	80
Active IPFE Migration	80
1 DAMP Migration	80 **Note:** DAMP time is based on the number of DAMPs and number of DAMPs in single cycle.
1 SBR Server Group Migration	240 **Note:** • Data migration is not considered. Data migration time is based on the number of sessions and binding. • The time mentioned here is for one SBR SG. Time is multiplied for number of SGs.

Table 2-1 (Cont.) Time Required for DSR Migration

Procedure	Time Required in minutes
KVM/Openstack Installation	120 **Note:** Installation and configuration time may vary based on the customer topology size.
KVM/Openstack configuration	120
Total	**1366**

2.2 Exporting Configuration Data on DSR 8.6.X

Export all the configuration data that is currently present on both NOAM and SOAM of 8.6.x DSR system.

Supported Applications to Export

Table 2-2 List of Supported Applications to Export on DSR NOAM

Keyword	Application Name
Diameter	Diameter
RADIUS	Radius
SBR	Subscriber Binding Repository
DCA	Diameter Custom Application
PCA	Policy and Charging Application

Table 2-3 List of Supported Applications to Export on DSR SOAM

Keyword	Application Name
Diameter	Diameter
IPFE	IP Front End
EIR	Equipment Identity Register
RADIUS	Radius
DCA	Diameter Custom Application
FABR	Full Address Based Resolution
PCA	Policy and Charging Application
RBAR	Range Based Address Resolution

Perform the following procedure to export configuration CSV file from DSR NOAM and SOAM.

1. Log in to DSR 8.6.X Active NOAM/SOAM GUI.
2. Navigate to **Diameter Common** from **Main Menu**, then select **Export**.

Figure 2-1 Exporting Diameter Common on NOAM

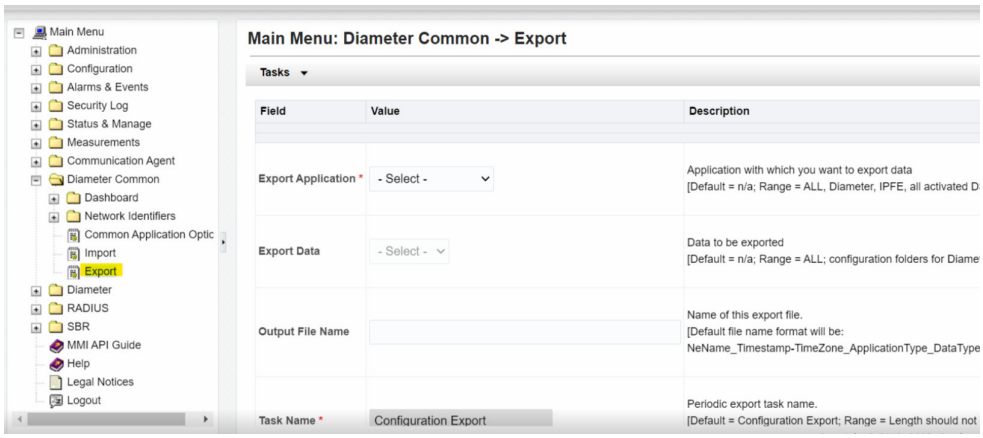
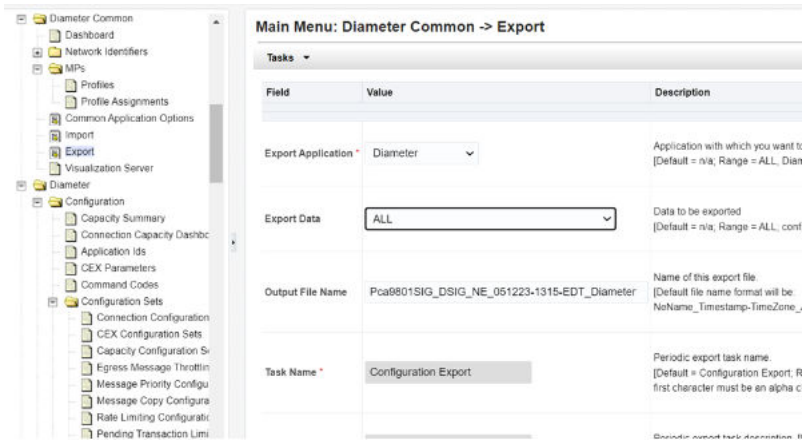


Figure 2-2 Exporting Diameter Common on SOAM



3. Update the required values for all the fields as mentioned in the following table and click **Ok** to confirm the configuration.

Table 2-4 Required Values to Export

Field Name	Value
Export Application	Select the required application from the drop-down list.
Export Data	Select **All** to export all the configuration csv files of the selected application. Else, it exports the configuration csv file to the particular table name selected.
Export Directory	Select **Export Server Directory** or **File Management Directory.** **Note:** Recommended value to use is **Export Server Directory**. The supported directory paths: • Export Server Directory Path: `/var/TKLC/db/filemgmt/export/<host_name>/DSR/<Application_name>` • File Management Directory Path: `/var/TKLC/db/filemgmt`
Export Frequency	Select value “One”.

3
Migration Checklist

This section describes migration tasks that are required to migrate from BM to VM.

Perform migration in the following sequence.

Table 3-1 Migration Sequence

Sequence	Task	Reference
1	Prerequisite	Prerequisites
2	Task - Standby NOAM	Shutting Down Standby BM NOAM
3	Task - Active NOAM	Migrating Standby BM NOAM to VM NOAM
4	Task - Standby SOAM	Migrating BM Standby SOAM to VM
5	Task - Active SOAM	Migrating BM Standby SOAM to VM
6	Task - Upgrade DAMPs	Migrating the DAMP Server
7	Task - Upgrade IPFEs	Identifying Standby IPFE Instance
8	Task - Upgrade SBR MPs	SBR Database Migration
9	Task - Migrate SDS	Refer to *SDS Migration Guide*.

3.1 Limitations

- For SBR MP migration, re-use of a IP address is not possible. Hence, additional hardware and additional IPs are required.
- While performing a complete migration, provisioning of new diameter configuration data is not recommended.
- In case of failure or any issues in VM deployments while reusing hardware, user cannot backout to 8.6.X release.

3.2 SBR Database Migration

Perform the following procedure to migrate SBR data.

1. Run the following command on Active and StandBy SOAM to verify if the value is 1.

   ```
   iqt -pE IdbParamDef where "param='IdbDisableUpgBarrier'"
   ```

   If value is 0, then run the following command:

   ```
   iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
   sudo init 6
   ```

2. Run the below command on all 8.6.x SBR servers in this order:
   a. Spare

b. Standby

c. Active

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

> **Note:**
>
> After restarting the server, wait till the server comes up and becomes serviceable. Then, run the above command on next server in the same server group.

3. Create new VMs for SBR Binding (Active, Standby and Spare).
4. Create new VMs for SBR Session (Active, Standby and Spare).
5. Add a new vDSR SBR-B/S in the existing path.
6. Create new server group for SBR-B/S consisting the vDSR 9.0.1 release.
7. Create new ResourceDomains for vDSR for both SBR-B/S.
8. Navigate to **Status & Manage** from **Main Menu**, then select **Server**. Click **Restart**, to enable the new vDSR SBR-B/S servers.
9. From Active NOAM, navigate to **Configuration** from **Main Menu: SBR**, then select **SBR Database Resizing Plans**.
10. Create new resizing plans for both binding and session. Keep BM SBR 8.6 as initial resource domain and vDSR 9.0.1 as target resource domain.
11. Navigate to **Maintenance** from **Main Menu: SBR**, then select **SBR Database Reconfiguration Status**.
12. Click **Prepare** for binding and session plan 1 by 1.
13. When status is in prepared state, click **Start** for binding and session resizing plan one after another.
14. Check if the vDSR SBR-B/S are created on all the new sessions and bindings.

    Wait for existing binding and sessions to be cleared from BM.
15. When resizing is complete, perform the following steps:
    - Remove BM SBR from the resource domain
    - Change SBR Binding or Session MP role to OOS
    - Remove BM SBR-B/S from Server group
    - Remove BM SBR-B/S from Server configuration

4
Migration

DSR 8.6.x BM can be migrated to vDSR 9.0.1 or later by using one of the following methods:

- Reuse of the Existing Hardware and Existing IP Addresses
- Reuse of the Existing Hardware and New IP Addresses
- New Hardware and Existing IP Addresses

4.1 Reuse of the Existing Hardware and Existing IP Addresses

This section describes migration process by shutting down existing NOAM, SOAM, IPFE, and DAMP on BM and deploying these applications on VM using the existing IP addresses.

4.1.1 Shutting Down Standby BM NOAM

Perform the following procedure to remove the standby NOAM from topology and shut down the standby NOAM on the DSR 8.6.x BM.

1. Remove standby NOAM from topology.
    a. Log in to DSR NOAM GUI using VIP.
    b. To change standby NOAM HA state to OOS, perform the following steps:
        i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
        ii. Click **Edit** and change **Max Allowed HA Role** of Standby NOAM to `OOS`.
    c. To remove the standby NOAM from NOAM Server group, perform the following steps:
        i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
        ii. Select **Noam (Level A)** Server Group and click **Edit**.
        iii. Uncheck **Standby Noam** from Server Group and click **OK**.
    d. Navigate to **Configuration** from **Main Menu**, then select **Servers** and select **Standby Noam**. Click **Delete.**
2. Shutdown standby NOAM by running the following command:

```
sudo shutdown -h now
```

4.1.2 Accessing XMI IP of DSR

Perform the following procedure to access and configure XMI IP of new vDSR 9.0.1 VM.

1. Install OL8 and KVM/OpenStack on the shutdown BM server.
2. Create DSR 9.0.1 VM.
3. Assign XMI IP to new vDSR 9.0.1 VM.

- To configure netmask and XMI IP address values, run the following command:

  ```
  sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --
  netmask=<netmask> --device=eth0 --address=<IP address>
  ```

  where, `<netmask>` indicates netmask of vDSR 9.0.1
  `<IP Address>` indicates the IP address of vDSR 9.0.1

> **Note:**
>
> For further information on accessing XMI IP, refer to *DSR Installation on OL8 and KVM* and *Software Installation Procedure* sections in *DSR Cloud Installation Guide*.

4.1.3 Configuring Network Element

Perform the following procedure to configure network element.

1. Log in to DSR 8.6.x Active NOAM GUI using VIP.
2. Export the network element configurations.
   a. Navigate to **Configuration** from **Main Menu**, then select **Networking** and click **Networks**.
   b. Select the required NOAM Network Element for configuration.
   c. Click **Export** and save the configuration.
3. Log in to NOAM vDSR 9.0.X GUI using XMI IP.
4. Configure Network Element for NOAM server on the vDSR 9.0.1.
   a. Navigate to **Configuration** from **Main Menu**, then select **Networking** and click **Networks**.
   b. Click **Browse** and select the file exported from the DSR 8.6.X server, to import the network element configuration.
   c. Click **Upload File**.
5. Configure server details on vDSR 9.0.1.
   a. Log in to 9.0.X vDSR instance GUI, which was created in the previous step.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. On **Insert** page, update the following server details:
      - Enter the standby NOAM hostname
      - Role as Network OAM&P
      - Hardware Profile as DSR Guest
      - Select the Noam Network element name
      - Configure XMI and IMI IP's and NTP server IP
   e. Click **Ok.**

6. Export and run `TKLCConfigData.sh` file on vDSR 9.0.1 NOAM.
   a. Log in to NOAM vDSR 9.0.X GUI using XMI IP.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Select the required NOAM server.
   d. Click **Export**, to export server configuration file to the file management folder on the NOAM.
   e. Perform `ssh` to XMI IP of the DSR 9.0.X VM.
   f. Run the `cd $FILE_MGMT_AREA/` command to access the file management area.
   g. Copy the `TKLCConfigData.sh` file to `/var/tmp` folder, by running the following command:

      ```
      cp TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh
      ```

   h. Verify the `/var/TKLC/appw/logs/Process/install.log` log file for successfully running the `TKLCCOnfigData.sh` file. You can run the following command to check logs.

      ```
      sudo tail -f /var/TKLC/appw/logs/Process/install.log
      ```

      Output:

      ```
      + sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
      bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e04
      f2e85fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g /usr/
      TKLC/appworks/prod/maint/loaders/install/postInstall/
      load.AppworksSecConfig
      + /usr/sbin/chpasswd
      ++ aw.wallet credential get tpdProvd tpdProvd
      + /usr/TKLC/appworks/sbin/updateMylogincnf
      Imysql: [Warning] Using a password on the command line interface can
      be insecure.
      Imysql: [Warning] Using a password on the command line interface can
      be insecure.
      + pm.kill apwSoapServer cmsoapa
      + /bin/touch /var/TKLC/appw/TKLCinitcfg
      + /bin/sleep 1
      [SUCCESS] script completed successfully! '
      ```

   i. Use the following command to update the `/etc/resolv.conf` file:

      ```
      sudo vim /etc/resolv.conf
      ```

   j. Add **IMI IP** of the **Active NOAM** at the end of file. Select **Save** and then **Close**.
      Sample `/etc/resolv.conf` file:

      ```
      [admusr@901noam00 ~]$ cat /etc/resolv.conf
      domain platform.cgbu.us.oracle.com
      nameserver 127.0.0.1
      nameserver 192.168.0.20     ; IMI IP of NOAM
      ```

7. Copy the `/var/named/db.platform.cgbu.us.oracle.com` from Active NOAM to vDSR 9.0.X NOAM, by running the following commands on DSR 9.0.X VM.

```
cd $FILE_MGMT_AREA/


sudo ssh admusr@<XMI ip of DSR 8.6.X> "sudo cat /var/named/
db.platform.cgbu.us.oracle.com " > db.platform.cgbu.us.oracle.com


sudo mv db.platform.cgbu.us.oracle.com /var/named/


sudo chown root:named /var/named/db.platform.cgbu.us.oracle.com


sudo chmod 640 /var/named/db.platform.cgbu.us.oracle.com
```

8. Wait for 10 minutes for server to configure the IP configuration, then reboot the VM using `sudo init 6` command on CLI.

4.1.4 Adding and Switching Over Standby NOAM Server

Perform the following procedure to add and switchover Standby NOAM server.

1. Add 9.0.X NOAM vDSR instance in the server group again on DSR 8.6.X Active NOAM, by performing the following steps:
   a. Log in to DSR 8.6.X Active NOAM GUI using VIP.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. Add the following details for vDSR 9.0.1 NOAM:
      - Enter NOAM hostname
      - Update Role as Network OAM&P
      - Hardware Profile as DSR Guest
      - Select the Noam Network element name
      - Configure XMI and IMI IP's and NTP server IP
   e. Click **Ok**.
   f. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
   g. Select the NOAM server group and click **Edit**.
   h. Select the 9.0.X vDSR Noam instance to add to the NOAM Server group. Then, click **Ok** to save the changes and wait for 5 minutes.
2. If the Max Allowed role of 9.0.X vDSR Noam instance is not Active, then navigate to **Status & Manage** from **Main Menu**, then select **HA**. Change Standby NOAM Max Allowed HA role to Active by clicking **Edit**.
3. Enable the Server, by performing the following steps:

a. ssh to vDSR 9.0.1 NOAM VM and run the following commands to disable the upgrade barrier feature:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

b. Log in to 8.6.X Active NOAM GUI using VIP.

c. Navigate to **Status & Manage** from **Main Menu**, then select **Server**.

d. Select Standby vDSR 9.0.X NOAM and click **Restart**.

4. To verify servers, perform the following steps:

a. Log in to the XMI IP of the vDSR 9.0.1.

b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.

c. Verify if the screen displays data for all the servers in the topology.

> **Note:**
>
> If this verification step fails, do not proceed further. For further help, contact My Oracle Support (MOS).

5. ssh to Standby vDSR 9.0.1 Noam and run the following command to check the HA state of the server:

```
ha.mystate -i
```

Output:

```
resourceId      role       node  DC           subResources     lastUpdate
-------------------------------------------------------------------------
-----
DbReplication   Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055749.923
          VIP   Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055749.925
CacdProcessRes  Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.583
CAPM_HELP_Proc  Act/OOS  BMtoVM-Migtest-DNO01         0
231003:055742.740
DSROAM_Proc     Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.585
CAPM_PSFS_Proc  Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055818.826
VSTPOAM_Proc    Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.584
VSTPSERVICE_Proc Act/OOS  BMtoVM-Migtest-DNO01        0
231003:055742.741
```

6. Run the following command, if any DSR application (such as PCA, FABR or RBAR) is activated and enabled on DSR.

   ```
   /usr/TKLC/dsr/bin/migrateNonReplicatedData
   ```

   > **Note:**
   >
   > This step is not required if none of the DSR applications are activated or enabled.

7. To switchover the role of Active NOAM to standby NOAM and standby NOAM to Active NOAM, perform the following steps:
   a. Log in to DSR 8.6.X Active NOAM GUI using XMI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA** and change **Max Allowed HA Role** of Active NOAM to Standby.

   > **Note:**
   >
   > Now vDSR NOAM instance is Active server and BM 8.6.X NOAM is Standby server.

4.1.5 Migrating Standby BM NOAM to VM NOAM

Perform the following procedure to migrate Standby BM NOAM to VM NOAM.

1. Remove standby NOAM from topology.
   a. Log in to Active DSR NOAM GUI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
   c. To change standby NOAM HA state to OOS, perform the following steps:
      i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
      ii. Click **Edit** and change **Max Allowed HA Role** of Standby NOAM to `OOS`.
   d. To remove the standby NOAM from NOAM Server group, perform the following steps:
      i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
      ii. Select **Noam (Level A)** Server Group and click **Edit**.
      iii. Uncheck **Standby Noam** from Server Group and click **OK**.
   e. Navigate to **Configuration** from **Main Menu**, then select **Servers** and select **Standby NOAM** and click **Delete**.
2. Shutdown standby NOAM by running the following command:

   ```
   sudo shutdown -h now
   ```

3. Install OL8 and KVM on the shutdown BM server.
4. Create vDSR 9.0.1 VM.

5. Assign XMI IP to new vDSR 9.0.1.
   - To configure netmask and XMI IP address values, run the following command:

     ```
     sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --netmask=<netmask> --
     device=eth0 --address=<IP address>
     ```

6. Add Standby NOAM server in the server group again on vDSR 9.0.1 Active NOAM, by performing the following steps:
   a. Log in to the XMI IP of the Active vDSR 9.0.1 VM server.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. Add the following details for NOAM server:
      - Enter NOAM hostname
      - Update Role as Network OAM&P
      - Hardware Profile as DSR Guest
      - Configure XMI and IMI IP's and NTP server IP
   e. Click **Ok**.
   f. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   g. Select new Standby NOAM server.
   h. Click **Export** to export server configuration file to filemgmt folder on the Active vDSR NOAM.
   i. Now ssh to Active DSR 9.0.X NOAM and follow the below steps to copy `TKLCConfigData.<hostname>.sh` to newly created Standby vDSR 9.0.1 NOAM. After copying the file, wait for 5 minutes.

      ```
      cd $FILE_MGMT_AREA


      sudo scp TKLCConfigData.<hostname>.sh admusr@<XMI IP of Standby
      NOAM>:/var/tmp/TKLCConfigData.sh
      ```

   j. Verify the `/var/TKLC/appw/logs/Process/install.log` log file on Standby NOAM for successfully running the `TKLCConfigData.sh` file. You can run following command to check logs.

      ```
      sudo tail -f /var/TKLC/appw/logs/Process/install.log
      ```

      Output:

      ```
      + sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
      bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e04
      f2e85fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g/usr/TKLC/
      appworks/prod/maint/loaders/install/postInstall/load.AppworksSecConfig
      + /usr/sbin/chpasswd
      ++ aw.wallet credential get tpdProvd tpdProvd
      + /usr/TKLC/appworks/sbin/updateMylogincnf
      Imysql: [Warning] Using a password on the command line interface can
      ```

```
be insecure.
Imysql: [Warning] Using a password on the command line interface
can be insecure.
+ pm.kill apwSoapServer cmsoapa
+ /bin/touch /var/TKLC/appw/TKLCinitcfg
+ /bin/sleep 1
[SUCCESS] script completed successfully!
```

k. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.

l. Select the **NOAM(Level A)** Server group and click **Edit**.

m. Select the standby NOAM to add to the NOAM Server group, then click **Ok** to save the changes and wait for 5 minutes.

n. If the Max Allowed HA Role of Standby NOAM is not Active, then navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of Standby NOAM to Active.

```
ssh to Standby DSR 9.0.X Noam
```

o. Run the following commands to disable the upgrade barrier feature:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

p. Log in to Active vDSR NOAM GUI.

q. Navigate to **Status & Manage** from **Main Menu**, then select **Server** and select Standby NOAM and click **Restart**.

7. To verify servers, perform the following steps:

   a. Log in to the VIP of the DSR 9.0.X NOAM VM.

   b. Navigate to **Status & Manage** from **Main Menu**, then select **Servers** and verify if the screen displays data for all the servers in the topology.

8. ssh to Standby 9.0.1 vDSR and run the following command, if any DSR application (such as PCA, FABR or RBAR) is activated and enabled on DSR.

```
/usr/TKLC/dsr/bin/migrateNonReplicatedData
```

> **Note:**
>
> - If this verification fails, contact My Oracle Support.
> - The `TKLCConfigData.sh` file must be copied using SCP from Active vDSR 9.0.1 NOAM server to the new vDSR 9.0.1 that is required to be configured as standby NOAM.

4.1.6 Updating the Database Table Values with vDSR 9.0.1 Value for NOAM

Perform the following procedure to update the database table values with vDSR 9.0.1 value for NOAM.

- Run following command on Active NOAM and Standby NOAM.

  ```
  /usr/TKLC/dsr/bin/updateConfigData 8.6
  ```

> **Note:**
>
> Ignore the following error while running on Standby NOAM.
>
> ```
> "disallowed write on replicated table"
> ```

4.1.7 Changing Max Allowed HA Role of Standby NOAM to Active

Perform the following procedure to update Max Allowed HA role of Standby NOAM to Active. If Max Allowed HA Role of Standby NOAM is not active, then perform this procedure.

1. Log in to the XMI IP of the Active NOAM vDSR 9.0.1.
2. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
3. Change Max Allowed HA Role of Standby Server to Active by clicking **Edit**.

4.1.8 Migrating BM Standby SOAM to VM

Perform the following procedure to migrate BM Standby SOAM to VM.

1. Remove standby SOAM from topology.
   a. Log in to Active DSR NOAM GUI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
   c. To change standby SOAM HA state to OOS, perform the following steps:
      i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
      ii. Click **Edit** and change **Max Allowed HA Role** of Standby SOAM to `OOS`.
   d. To remove the standby SOAM from SOAM Server group, perform the following steps:
      i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
      ii. Select **SOAM (Level B)** Server Group and click **Edit**.
      iii. Uncheck **Standby SOAM** from Server Group and click **OK**.
   e. Navigate to **Configuration** from **Main Menu**, then select **Servers** and select **Standby SOAM** and click **Delete**.

2. Shutdown standby SOAM by running the following command:

   ```
   sudo shutdown -h now
   ```

3. Install OL8 and KVM on the shutdown BM server.

   > **Note:**
   >
   > For information on installing OL8 and KVM, refer to *DSR Installation on OL8 and KVM* section in *DSR Cloud Installation Guide*.

4. Create vDSR 9.0.1 VM.

   > **Note:**
   >
   > Create SOAM VM where Active NOAM VM is created.

5. Assign XMI IP to new vDSR 9.0.1.
   - To configure netmask and XMI IP address values, run the following command:

     ```
     sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --
     netmask=<netmask> --device=eth0 --address=<IP address>
     ```

6. Export and run `TKLCConfigData.sh` file of Standby SOAM.
   a. Log in to VIP IP of the DSR 9.0.X Active NOAM VM.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. Add the following details for SOAM server:
      - Enter SOAM hostname
      - Update Role as System OAM
      - Hardware Profile as DSR Guest
      - Configure XMI and IMI IP's and NTP server IP
   e. Click **Ok**.
   f. Select the required standby SOAM server, which was created in the previous step.
   g. Click **Export**, to export server configuration file to the file management folder on the Active NOAM.

h. Now ssh to Active DSR 9.0.X NOAM and copy `TKLCConfigData.<hostname>.sh` file to the newly created vDSR 9.0.X SOAM. After copying the file wait for 5 minutes.

```
cd $FILE_MGMT_AREA


sudo scp TKLCConfigData.<hostname>.sh admusr@<XMI IP of new vDSR
9.0.X SOAM VM>:/var/tmp/TKLCConfigData.sh
```

i. SSH to the new vDSR 9.0.X SOAM VM IP and verify the `/var/TKLC/appw/logs/Process/install.log` log file for successfully running of `TKLCConfigData.sh` file. You can run following command to check logs.

```
sudo tail -f /var/TKLC/appw/logs/Process/install.log
```

Output:

```
+ sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e04
f2e85fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g/usr/TKLC/
appworks/prod/maint/loaders/install/postInstall/load.AppworksSecConfig
+ /usr/sbin/chpasswd
++ aw.wallet credential get tpdProvd tpdProvd
+ /usr/TKLC/appworks/sbin/updateMylogincnf
Imysql: [Warning] Using a password on the command line interface can
be insecure.
Imysql: [Warning] Using a password on the command line interface can
be insecure.
+ pm.kill apwSoapServer cmsoapa
+ /bin/touch /var/TKLC/appw/TKLCinitcfg
+ /bin/sleep 1
[SUCCESS] script completed successfully!
```

j. Wait for 10 minutes for server to configure with the IP configuration, then reboot the VM using `sudo init 6` command on CLI.

k. Log in to Active DSR NOAM GUI using VIP.

l. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.

m. Select the **SOAM(Level B)** Server group and click **Edit**.

n. Select the new vDSR 9.0.X SOAM VM to add to the SOAM Server group, then click **Ok** to save the changes and wait for 5 minutes.

> **Note:**
>
> After adding new vDSR 9.0.X SOAM VM to SOAM Server group it is configured as Standby SOAM. Post that the newly added vDSR 9.0.X SOAM VM will be considered as Standby SOAM.

o. If the Max Allowed HA Role of the new vDSR 9.0.X SOAM VM is not Active then navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of the new vDSR 9.0.X SOAM VM to Active.

p. ssh to Standby DSR 9.0.X SOAM.

q. Run the following commands to disable the upgrade barrier feature:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

r. Log in to Active vDSR Noam GUI.

s. Navigate to **Status & Manage** from **Main Menu**, then select **Server** and select Standby SOAM and click **Restart**.

7. ssh to Standby 9.0.1 vDSR SOAM and run the following command, if any DSR application (such as PCA, FABR or RBAR) is activated and enabled on DSR.

```
/usr/TKLC/dsr/bin/migrateNonReplicatedData
```

> **Note:**
>
> This step is not required if none of the DSR applications are activated or enabled.

8. To switchover the role of Active SOAM to standby SOAM and standby SOAM to Active SOAM, perform the following steps:

a. Log in to DSR 9.0.1 Active NOAM VIP.

b. Navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of Active SOAM HA state to Standby.

9. After switching over, the Standby vDSR 9.0.X VM will be Active and 8.6.X DSR BM NOAM will be Standby.

   Repeat the steps in Migrating BM Standby SOAM to VM to migrate the 8.6.X BM standby SOAM to 9.0.X.

4.1.9 Updating the Database Table Values with vDSR 9.0.1 Value for SOAM

Perform the following procedure to update the database table values with vDSR 9.0.1 value for SOAM.

- Run following command on Active SOAM and Standby SOAM.

```
/usr/TKLC/dsr/bin/updateConfigData 8.6
```

> **Note:**
>
> Ignore the following error while running on Standby SOAM.
>
> ```
> "disallowed write on replicated table"
> ```

4.1.10 Migrating the DAMP Server

Perform the below steps to migrate 8.6.X DAMP BM to 9.0.X VM.

> **Note:**
>
> This procedure can be performed on 20% of DAMPs at once.

1. Remove DAMP from topology.
   a. Log in to Active NOAM DSR GUI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
   c. To change HA state of DAMP to Out of Service (OOS), perform the following steps:
      i. To change DAMP HA state to OOS, perform the following steps:
         i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
         ii. Click **Edit** and change **Max Allowed HA Role** of DAMP to `OOS`.
      ii. To remove the DAMP instance from DAMP Server group, perform the following steps:
         i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
         ii. Select **DAMP (Level C)** Server Group and click **Edit**.
         iii. Uncheck the required DAMP instance from Server Group and click **OK**.
      iii. Navigate to **Configuration** from **Main Menu**, then select **Servers**. Then, select the DAMP instance which was removed from server group in last step and click **Delete**.
2. Shut down DAMP by running the following command:

   ```
   sudo shutdown -h now
   ```

3. Install OL8 and KVM on the shutdown BM server.
4. Create vDSR 9.0.1.

   > **Note:**
   >
   > Create DAMP on the same host where NOAM, SOAM VM was created.

5. Assign XMI IP to new vDSR 9.0.1.

   To configure netmask and XMI IP address values, run the following command:

   ```
   sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --netmask=<netmask> --
   device=eth0 --address=<IP address>
   ```

6. Log in to DSR Active vDSR 9.0.1 NOAM using XMI.
7. Navigate to **Configuration** from **Main Menu**, then select **Servers**.

8. Click **Insert**.
9. Add the following details for DAMP server:
   - Enter DAMP hostname
   - Update Role as MP
   - Hardware Profile as DSR Guest
   - Configure XMI and IMI, XSI IP's and NTP server IP
10. Click **Ok**.
11. Select the required DAMP server (which was created in the previous step).
12. Click **Export**, to export server configuration file to the file management folder on the Active NOAM.
13. Now ssh to Active DSR 9.0.X NOAM and copy the `TKLCConfigData.<hostname>.sh` file to the DAMP. After copying the file wait for 5 minutes.

    ```
    cd $FILE_MGMT_AREA


    sudo scp TKLCConfigData.<hostname>.sh admusr@<XMI IP of newly added
    vDSR DAMP>:/var/tmp/TKLCConfigData.sh
    ```

14. ssh to DAMP XMI IP and verify the `/var/TKLC/appw/logs/Process/install.log` log file for successfully running of `TKLCConfigData.sh` file. You can run following command to check logs.

    ```
    sudo tail -f /var/TKLC/appw/logs/Process/install.log
    ```

    Output:

    ```
    + sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
    bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e
    04f2e85fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g/usr/
    TKLC/appworks/prod/maint/loaders/install/postInstall/
    load.AppworksSecConfig
    + /usr/sbin/chpasswd
    ++ aw.wallet credential get tpdProvd tpdProvd
    + /usr/TKLC/appworks/sbin/updateMylogincnf
    Imysql: [Warning] Using a password on the command line interface
    can be insecure.
    Imysql: [Warning] Using a password on the command line interface
    can be insecure.
    + pm.kill apwSoapServer cmsoapa
    + /bin/touch /var/TKLC/appw/TKLCinitcfg
    + /bin/sleep 1
    [SUCCESS] script completed successfully!
    ```

15. Wait for 10 minutes for server to configure with the IP configuration, then reboot the VM using `sudo init 6` command on CLI.
16. Log in to Active vDSR NOAM GUI.

17. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
18. Select the **DAMP (Level C)** Server group and click **Edit**.
19. Select the DAMP instance, which was added while updating DAMP server details, to add to the DAMP Server group. Click **Ok** to save the changes and wait for 5 minutes.
20. If the Max Allowed HA Role of that DAMP instance, which was added to server group in previous step, is not Active then navigate to **Status & Manage** from **Main Menu**. Then, select **HA** and change Max Allowed HA Role of DAMP to Active.
21. ssh to newly added vDSR 9.0.X DAMP.
22. Run the following commands to disable the upgrade barrier feature:

    ```
    iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
    sudo init 6
    ```

23. Log in to Active vDSR NOAM GUI.
24. Navigate to **Status & Manage** from **Main Menu**, then select **Server** and select the newly added DAMP instance. Click **Restart**.
25. Run following command on DAMP:

    ```
    /usr/TKLC/dsr/bin/updateConfigData 8.6
    ```

> **Note:**
>
> - Ignore the following error while running on DAMP error:
>
>   ```
>   "disallowed write on replicated table"
>   ```
>
> - To configure remaining DAMPs, repeat procedure Migrating the DAMP Server for each 20% of DAMP until you reach 100% of DAMP server.
> - DAMP leader must be migrated last. DC and MP leaders should not be planned in the same migration cycle.

4.1.11 Identifying Standby IPFE Instance

Perform the following procedure to find the Standby IPFE instance.

1. On Active SOAM GUI, navigate to **IPFE** from **Main Menu**, then select **Configuration** and click **Target Sets**.
2. Select the preferred Active IPFE for a Target Set.
   - If IPFE-A1 is mentioned in preferred Active for target set, then IPFE-A2 is standby and vice-versa
   - if IPFE B1 is mentioned in preferred Active for target set, then IPFE-B2 is standby and vice-versa
3. Assume that IPFE-A2 is standby from the above steps.
4. On Active SOAM GUI, navigate to **IPFE** from **Main Menu**, then select **Configuration** and click **Options**.

5. Check which instance IP is mentioned in IPFE-A2 configuration and consider that IPFE instance is Standby IPFE.

4.1.12 Migrating Standby BM IPFE on VM

Perform the following procedure to migrate Standby BM IPFE on VM.

1. Remove Standby IPFE from topology.
   a. Log in to Active NOAM DSR GUI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
   c. To change HA state of IPFE to Out of Service (OOS), perform the following steps:
      i. To change IPFE HA state to OOS, perform the following steps:
         i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
         ii. Click **Edit** and change **Max Allowed HA Role** of IPFE to `OOS`.
      ii. To remove the standby IPFE from IPFE Server group, perform the following steps:
         i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
         ii. Select Server Group which contains Standby IPFE instance and click **Edit**.
         iii. Uncheck Standby IPFE instance from Server Group and click **OK**.
      iii. Navigate to **Configuration** from **Main Menu**, then select **Servers** and select Standby IPFE. Click **Delete**.
2. Shutdown IPFE by running the following command:

   ```
   sudo shutdown -h now
   ```

3. Install OL8 and KVM on the shutdown BM server.
4. Create vDSR 9.0.1.

   > **Note:**
   >
   > Create IPFE on the same host where DAMP, SOAM, NOAM VM was created.

5. Assign XMI IP to new vDSR 9.0.1.

   To configure netmask and XMI IP address values, run the following command:

   ```
   sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --netmask=<netmask>
   --device=eth0 --address=<IP address>
   ```

6. Log in to DSR Active vDSR 9.0.1 NOAM using XMI.
7. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
8. Click **Insert**.

9. Add the following details for IPFE server:
   - Enter IPFE hostname
   - Update Role as MP
   - Hardware Profile as DSR Guest
   - Configure XMI and IMI, XSI IP's and NTP server IP
10. Click **Ok**.
11. Select the required IPFE server (which was created in the previous step).
12. Click **Export**, to export server configuration file to the file management folder on the Active NOAM.
13. Now ssh to Active DSR 9.0.X NOAM and copy the `TKLCConfigData.<hostname>.sh` file to the IPFE. After copying the file wait for 5 minutes.

    ```
    cd $FILE_MGMT_AREA


    sudo scp TKLCConfigData.<hostname>.sh admusr@<XMI IP of new vDSR IPFE
    instance>:/var/tmp/TKLCConfigData.sh
    ```

14. ssh to IPFE XMI IP and verify the `/var/TKLC/appw/logs/Process/install.log` log file for successfully running of `TKLCConfigData.sh` file. You can run following command to check logs.

    ```
    sudo tail -f /var/TKLC/appw/logs/Process/install.log
    ```

    Output:

    ```
    + sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
    bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e04f2e8
    5fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g/usr/TKLC/
    appworks/prod/maint/loaders/install/postInstall/load.AppworksSecConfig
    + /usr/sbin/chpasswd
    ++ aw.wallet credential get tpdProvd tpdProvd
    + /usr/TKLC/appworks/sbin/updateMylogincnf
    Imysql: [Warning] Using a password on the command line interface can be
    insecure.
    Imysql: [Warning] Using a password on the command line interface can be
    insecure.
    + pm.kill apwSoapServer cmsoapa
    + /bin/touch /var/TKLC/appw/TKLCinitcfg
    + /bin/sleep 1
    [SUCCESS] script completed successfully!
    ```

15. Wait for 10 minutes for server to configure with the IP configuration, then reboot the VM using `sudo init 6` command on CLI.
16. Log in to Active vDSR NOAM GUI.
17. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
18. Select the IPFE (Level C) Server group and click **Edit**.

> **Note:**
>
> Add IPFE to the same server group from where IPFE was removed.

19. Select the newly added vDSR IPFE instance to add to the IPFE Server group, then click **Ok** to save the changes and wait for 5 minutes.
20. If the Max Allowed HA Role of new vDSR IPFE is not Active then navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of that IPFE instance to Active.
21. SSH to newly added vDSR IPFE instance.
22. Run the following commands to disable the upgrade barrier feature:

    ```
    iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
    sudo init 6
    ```

23. Log in to Active vDSR NOAM GUI.
24. Navigate to **Status & Manage** from **Main Menu**, then select **Server** and select **IPFE**. Click **Restart**.
25. Run following command on newly added vDSR IPFE instance:

    ```
    /usr/TKLC/dsr/bin/updateConfigData 8.6
    ```

> **Note:**
>
> Ignore the following error while running on IPFE error:
>
> ```
> "disallowed write on replicated table"
> ```

4.1.13 Configuring IPFE from SOAM

Perform the following procedure to configure IPFE from SOAM.

- Modify the IPFE options from SOAM.

> **Note:**
>
> These changes are required if IPFE XMI and IMI ip addresses are changed. If IMI and XMI IP addresses are re-used, this step is not required.

1. From Active SOAM GUI, navigate to **IPFE** from **Main Menu**, then select **Configuration** and click **Options**.
2. Configure the IPFE-A1/A2/B1/B2 section, which was considered as Standby.

4.1.14 Switching Over IPFE

Perform the following procedure to switch over IPFE.

1. Add Standby NOAM server in the server group again on DSR 8.6.X Active NOAM, by performing the following steps:
   a. Log in to the VIP of the DSR 8.6.X Active NOAM server.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. Add the following details for NOAM server:
      - Enter NOAM hostname
      - Update Role as Network OAM&P
      - Hardware Profile as DSR Guest
      - Select the NOAM Network element name
      - Configure XMI, IMI IP's, and NTP server IP
   e. Click **Ok**.
   f. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
   g. Select the NOAM server group and click **Edit**.
   h. Select the standby NOAM to add to the NOAM Server group, then click **Ok** to save the changes. Then, wait for 5 minutes.
2. If the Max Allowed HA role for Standby NOAM is not Active, then navigate to **Status & Manage** from **Main Menu**. Select **HA** and change Standby NOAM Max Allowed HA role to Active by clicking **Edit**.
   a. ssh to vDSR 9.0.1 VM and Run the following commands to disable the upgrade barrier feature:

      ```
      iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
      sudo init 6
      ```

   b. Log in to Active NOAM GUI.
   c. Navigate to **Status & Manage** from **Main Menu**, then select **Server**, then select Standby NOAM server and click **Restart**.
3. To verify servers, perform the following steps:
   a. Log in to the XMI IP of the vDSR 9.0.1.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**. Then, verify if the screen displays data for all the servers in the topology.

   > **Note:**
   >
   > If this verification step fails, do not proceed further. For further help, contact My Oracle Support (MOS).

4. ssh to Standby vDSR 9.0.1 NOAM.

5. Run the following command to check the HA state of the server:

```
ha.mystate -i
```

Output:

```
resourceId      role          node  DC        subResources
lastUpdate
-------------------------------------------------------------------
----------------------
DbReplication   Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055749.923
VIP             Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055749.925
CacdProcessRes  Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.583
CAPM_HELP_Proc  Act/OOS  BMtoVM-Migtest-DNO01         0
231003:055742.740
DSROAM_Proc     Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.585
CAPM_PSFS_Proc  Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055818.826
VSTPOAM_Proc    Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.584
VSTPSERVICE_Proc Act/OOS  BMtoVM-Migtest-DNO01        0
231003:055742.741
```

6. Run the following command, if any DSR application (such as PCA, FABR or RBAR) is activated and enabled on DSR.

```
/usr/TKLC/dsr/bin/migrateNonReplicatedData
```

> **Note:**
>
> This step is not required if none of the DSR applications are activated or enabled.

7. To switchover the role of Active NOAM to standby NOAM and standby NOAM to Active NOAM, perform the following steps:
   a. Log in to DSR 8.6.X BM Server using XMI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of Active NOAM to Standby.

4.2 Reuse of the Existing Hardware and New IP Addresses

This section describes migration process by shutting down existing NOAM, SOAM, IPFE, and DAMP on BM and deploying these new NOAM, SOAM, IPFE, and DAMP, on VM using new IP addresses.

> **Note:**
>
> For method 2, use the new IP addresses for existing hardware and perform the procedure mentioned in Reuse of the Existing Hardware and Existing IP Addresses.

4.3 New Hardware and Existing IP Addresses

This section describes migration process by shutting down existing NOAM, SOAM, IPFE, and DAMP on BM and deploying these new NOAM, SOAM, IPFE, and DAMP, on VM using existing IP addresses.

Prerequisites:

- Before starting migration, create new VM's on the new hardware.

4.3.1 Shutting Down Standby BM NOAM

Perform the following procedure to remove the standby NOAM from topology and shut down the standby NOAM on the DSR 8.6.x BM.

1. Remove standby NOAM from topology.
   a. Log in to DSR NOAM GUI using VIP.
   b. To change standby NOAM HA state to OOS, perform the following steps:
      i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
      ii. Click **Edit** and change **Max Allowed HA Role** of Standby NOAM to `OOS`.
   c. To remove the standby NOAM from NOAM Server group, perform the following steps:
      i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
      ii. Select **Noam (Level A)** Server Group and click **Edit**.
      iii. Uncheck **Standby Noam** from Server Group and click **OK**.
   d. Navigate to **Configuration** from **Main Menu**, then select **Servers** and select **Standby Noam**. Click **Delete.**
2. Shutdown standby NOAM by running the following command:

   ```
   sudo shutdown -h now
   ```

4.3.2 Accessing XMI IP of DSR

Perform the following procedure to access and configure XMI IP of new vDSR 9.0.1 VM.

- Assign XMI IP to new vDSR 9.0.1 VM.
  - To configure netmask and XMI IP address values, run the following command:

    ```
    sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --netmask=<netmask> --
    device=eth0 --address=<IP address>
    ```

    where, `<netmask>` indicates netmask of vDSR 9.0.1

`<IP Address>` indicates the IP address of vDSR 9.0.1

> **Note:**
>
> For further information on accessing XMI IP, refer to *DSR Installation on OL8 and KVM* and *Software Installation Procedure* sections in *DSR Cloud Installation Guide*.

4.3.3 Configuring Network Element

Perform the following procedure to configure network element.

1. Log in to DSR 8.6.x Active NOAM GUI using VIP.
2. Export the network element configurations.
   a. Navigate to **Configuration** from **Main Menu**, then select **Networking** and click **Networks**.
   b. Select the required NOAM Network Element for configuration.
   c. Click **Export** and save the configuration.
3. Log in to NOAM vDSR 9.0.X GUI using XMI IP.
4. Configure Network Element for NOAM server on the vDSR 9.0.1.
   a. Navigate to **Configuration** from **Main Menu**, then select **Networking** and click **Networks**.
   b. Click **Browse** and select the file exported from the DSR 8.6.X server, to import the network element configuration.
   c. Click **Upload File**.
5. Configure server details on vDSR 9.0.1.
   a. Log in to 9.0.X vDSR instance GUI, which was created in the previous step.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. On **Insert** page, update the following server details:
      - Enter the standby NOAM hostname
      - Role as Network OAM&P
      - Hardware Profile as DSR Guest
      - Select the Noam Network element name
      - Configure XMI and IMI IP's and NTP server IP
   e. Click **Ok.**
6. Export and run `TKLCConfigData.sh` file on vDSR 9.0.1 NOAM.
   a. Log in to NOAM vDSR 9.0.X GUI using XMI IP.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Select the required NOAM server.

d. Click **Export**, to export server configuration file to the file management folder on the NOAM.

e. Perform `ssh` to XMI IP of the DSR 9.0.X VM.

f. Run the `cd $FILE_MGMT_AREA/` command to access the file management area.

g. Copy the `TKLCConfigData.sh` file to `/var/tmp` folder, by running the following command:

```
cp TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh
```

h. Verify the `/var/TKLC/appw/logs/Process/install.log` log file for successfully running the `TKLCCOnfigData.sh` file. You can run the following command to check logs.

```
sudo tail -f /var/TKLC/appw/logs/Process/install.log
```

Output:

```
+ sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e04
f2e85fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g /usr/
TKLC/appworks/prod/maint/loaders/install/postInstall/
load.AppworksSecConfig
+ /usr/sbin/chpasswd
++ aw.wallet credential get tpdProvd tpdProvd
+ /usr/TKLC/appworks/sbin/updateMylogincnf
Imysql: [Warning] Using a password on the command line interface can
be insecure.
Imysql: [Warning] Using a password on the command line interface can
be insecure.
+ pm.kill apwSoapServer cmsoapa
+ /bin/touch /var/TKLC/appw/TKLCinitcfg
+ /bin/sleep 1
[SUCCESS] script completed successfully! '
```

i. Use the following command to update the `/etc/resolv.conf` file:

```
sudo vim /etc/resolv.conf
```

j. Add **IMI IP** of the **Active NOAM** at the end of file. Select **Save** and then **Close**. **Sample `/etc/resolv.conf` file:**

```
[admusr@901noam00 ~]$ cat /etc/resolv.conf
domain platform.cgbu.us.oracle.com
nameserver 127.0.0.1
nameserver 192.168.0.20     ; IMI IP of NOAM
```

7. Copy the `/var/named/db.platform.cgbu.us.oracle.com` from Active NOAM to vDSR 9.0.X NOAM, by running the following commands on DSR 9.0.X VM.

```
cd $FILE_MGMT_AREA/


sudo ssh admusr@<XMI ip of DSR 8.6.X> "sudo cat /var/named/
db.platform.cgbu.us.oracle.com " > db.platform.cgbu.us.oracle.com


sudo mv db.platform.cgbu.us.oracle.com /var/named/


sudo chown root:named /var/named/db.platform.cgbu.us.oracle.com


sudo chmod 640 /var/named/db.platform.cgbu.us.oracle.com
```

8. Wait for 10 minutes for server to configure the IP configuration, then reboot the VM using `sudo init 6` command on CLI.

4.3.4 Adding and Switching Over Standby NOAM Server

Perform the following procedure to add and switchover Standby NOAM server.

1. Add 9.0.X NOAM vDSR instance in the server group again on DSR 8.6.X Active NOAM, by performing the following steps:
   a. Log in to DSR 8.6.X Active NOAM GUI using VIP.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. Add the following details for vDSR 9.0.1 NOAM:
      - Enter NOAM hostname
      - Update Role as Network OAM&P
      - Hardware Profile as DSR Guest
      - Select the Noam Network element name
      - Configure XMI and IMI IP's and NTP server IP
   e. Click **Ok**.
   f. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
   g. Select the NOAM server group and click **Edit**.
   h. Select the 9.0.X vDSR Noam instance to add to the NOAM Server group. Then, click **Ok** to save the changes and wait for 5 minutes.
2. If the Max Allowed role of 9.0.X vDSR Noam instance is not Active, then navigate to **Status & Manage** from **Main Menu**, then select **HA**. Change Standby NOAM Max Allowed HA role to Active by clicking **Edit**.
3. Enable the Server, by performing the following steps:

a. ssh to vDSR 9.0.1 NOAM VM and run the following commands to disable the upgrade barrier feature:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

b. Log in to 8.6.X Active NOAM GUI using VIP.

c. Navigate to **Status & Manage** from **Main Menu**, then select **Server**.

d. Select Standby vDSR 9.0.X NOAM and click **Restart**.

4. To verify servers, perform the following steps:

a. Log in to the XMI IP of the vDSR 9.0.1.

b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.

c. Verify if the screen displays data for all the servers in the topology.

> **Note:**
>
> If this verification step fails, do not proceed further. For further help, contact My Oracle Support (MOS).

5. ssh to Standby vDSR 9.0.1 NOAM and run the following command to check the HA state of the server:

```
ha.mystate -i
```

Output:

```
resourceId      role       node  DC           subResources     lastUpdate
-------------------------------------------------------------------------
-----
DbReplication   Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055749.923
          VIP   Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055749.925
CacdProcessRes  Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.583
CAPM_HELP_Proc  Act/OOS  BMtoVM-Migtest-DNO01         0
231003:055742.740
DSROAM_Proc     Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.585
CAPM_PSFS_Proc  Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055818.826
VSTPOAM_Proc    Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.584
VSTPSERVICE_Proc Act/OOS  BMtoVM-Migtest-DNO01        0
231003:055742.741
```

6. Run the following command, if any DSR application (such as PCA, FABR or RBAR) is activated and enabled on DSR.

   ```
   /usr/TKLC/dsr/bin/migrateNonReplicatedData
   ```

   > **Note:**
   >
   > This step is not required if none of the DSR applications are activated or enabled.

7. To switchover the role of Active NOAM to standby NOAM and standby NOAM to Active NOAM, perform the following steps:
   a. Log in to DSR 8.6.X Active NOAM GUI using XMI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA** and change **Max Allowed HA Role** of Active NOAM to Standby.

      > **Note:**
      >
      > Now vDSR NOAM instance is Active server and BM 8.6.X NOAM is Standby server.

4.3.5 Migrating Standby BM NOAM to VM NOAM

Perform the following procedure to migrate Standby BM NOAM to VM NOAM.

1. Remove standby NOAM from topology.
   a. Log in to Active DSR NOAM GUI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
   c. To change standby NOAM HA state to OOS, perform the following steps:
      i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
      ii. Click **Edit** and change **Max Allowed HA Role** of Standby NOAM to `OOS`.
   d. To remove the standby NOAM from NOAM Server group, perform the following steps:
      i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
      ii. Select **Noam (Level A)** Server Group and click **Edit**.
      iii. Uncheck **Standby Noam** from Server Group and click **OK**.
   e. Navigate to **Configuration** from **Main Menu**, then select **Servers** and select **Standby NOAM** and click **Delete**.
2. Shutdown standby NOAM by running the following command:

   ```
   sudo shutdown -h now
   ```

3. Create vDSR 9.0.1 VM.
4. Assign XMI IP to new vDSR 9.0.1.

- To configure netmask and XMI IP address values, run the following command:

  ```
  sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --netmask=<netmask> --
  device=eth0 --address=<IP address>
  ```

5. Add Standby NOAM server in the server group again on vDSR 9.0.1 Active NOAM, by performing the following steps:
   a. Log in to the XMI IP of the Active vDSR 9.0.1 VM server.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. Add the following details for NOAM server:
      - Enter NOAM hostname
      - Update Role as Network OAM&P
      - Hardware Profile as DSR Guest
      - Configure XMI and IMI IP's and NTP server IP
   e. Click **Ok**.
   f. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   g. Select new Standby NOAM server.
   h. Click **Export** to export server configuration file to filemgmt folder on the Active vDSR NOAM.
   i. Now ssh to Active DSR 9.0.X NOAM and follow the below steps to copy `TKLCConfigData.<hostname>.sh` to newly created Standby vDSR 9.0.1 NOAM. After copying the file, wait for 5 minutes.

      ```
      cd $FILE_MGMT_AREA


      sudo scp TKLCConfigData.<hostname>.sh admusr@<XMI IP of Standby
      NOAM>:/var/tmp/TKLCConfigData.sh
      ```

   j. Verify the `/var/TKLC/appw/logs/Process/install.log` log file on Standby NOAM for successfully running the `TKLCConfigData.sh` file. You can run following command to check logs.

      ```
      sudo tail -f /var/TKLC/appw/logs/Process/install.log
      ```

      Output:

      ```
      + sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
      bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e04
      f2e85fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g/usr/TKLC/
      appworks/prod/maint/loaders/install/postInstall/load.AppworksSecConfig
      + /usr/sbin/chpasswd
      ++ aw.wallet credential get tpdProvd tpdProvd
      + /usr/TKLC/appworks/sbin/updateMylogincnf
      Imysql: [Warning] Using a password on the command line interface can
      be insecure.
      ```

```
Imysql: [Warning] Using a password on the command line interface
can be insecure.
+ pm.kill apwSoapServer cmsoapa
+ /bin/touch /var/TKLC/appw/TKLCinitcfg
+ /bin/sleep 1
[SUCCESS] script completed successfully!
```

k. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.

l. Select the **NOAM(Level A)** Server group and click **Edit**.

m. Select the standby NOAM to add to the NOAM Server group, then click **Ok** to save the changes and wait for 5 minutes.

n. If the Max Allowed HA Role of Standby NOAM is not Active, then navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of Standby NOAM to Active.

```
ssh to Standby DSR 9.0.X Noam
```

o. Run the following commands to disable the upgrade barrier feature:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

p. Log in to Active vDSR NOAM GUI.

q. Navigate to **Status & Manage** from **Main Menu**, then select **Server** and select Standby NOAM and click **Restart**.

6. To verify servers, perform the following steps:

   a. Log in to the VIP of the DSR 9.0.X NOAM VM.

   b. Navigate to **Status & Manage** from **Main Menu**, then select **Servers** and verify if the screen displays data for all the servers in the topology.

7. ssh to Standby 9.0.1 vDSR and run the following command, if any DSR application (such as PCA, FABR or RBAR) is activated and enabled on DSR.

```
/usr/TKLC/dsr/bin/migrateNonReplicatedData
```

> **Note:**
>
> - If this verification fails, contact My Oracle Support.
> - The `TKLCConfigData.sh` file must be copied using SCP from Active vDSR 9.0.1 NOAM server to the new vDSR 9.0.1 that is required to be configured as standby NOAM.

4.3.6 Updating the Database Table Values with vDSR 9.0.1 Value for NOAM

Perform the following procedure to update the database table values with vDSR 9.0.1 value for NOAM.

- Run following command on Active NOAM and Standby NOAM.

  ```
  /usr/TKLC/dsr/bin/updateConfigData 8.6
  ```

> **Note:**
>
> Ignore the following error while running on Standby NOAM.
>
> ```
> "disallowed write on replicated table"
> ```

4.3.7 Changing Max Allowed HA Role of Standby NOAM to Active

Perform the following procedure to update Max Allowed HA role of Standby NOAM to Active. If Max Allowed HA Role of Standby NOAM is not active, then perform this procedure.

1. Log in to the XMI IP of the Active NOAM vDSR 9.0.1.
2. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
3. Change Max Allowed HA Role of Standby Server to Active by clicking **Edit**.

4.3.8 Migrating BM Standby SOAM to VM

Perform the following procedure to migrate BM Standby SOAM to VM.

1. Remove standby SOAM from topology.
   a. Log in to Active DSR NOAM GUI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
   c. To change standby SOAM HA state to OOS, perform the following steps:
      i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
      ii. Click **Edit** and change **Max Allowed HA Role** of Standby SOAM to `OOS`.
   d. To remove the standby SOAM from SOAM Server group, perform the following steps:
      i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
      ii. Select **SOAM (Level B)** Server Group and click **Edit**.
      iii. Uncheck **Standby SOAM** from Server Group and click **OK**.
   e. Navigate to **Configuration** from **Main Menu**, then select **Servers** and select **Standby SOAM** and click **Delete**.

2. Shutdown standby SOAM by running the following command:

   ```
   sudo shutdown -h now
   ```

3. Create vDSR 9.0.1 VM.

   > **Note:**
   >
   > Create SOAM VM where Active NOAM VM is created.

4. Assign XMI IP to new vDSR 9.0.1 VM.
   - To configure netmask and XMI IP address values, run the following command:

     ```
     sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --
     netmask=<netmask> --device=eth0 --address=<IP address>
     ```

5. Export and run `TKLCConfigData.sh` file of Standby SOAM.
   a. Log in to VIP IP of the DSR 9.0.X Active NOAM VM.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.
   d. Add the following details for SOAM server:
      - Enter SOAM hostname
      - Update Role as System OAM
      - Hardware Profile as DSR Guest
      - Configure XMI and IMI IP's and NTP server IP
   e. Click **Ok**.
   f. Select the required standby SOAM server, which was created in the previous step.
   g. Click **Export**, to export server configuration file to the file management folder on the Active NOAM.
   h. Now ssh to Active DSR 9.0.X NOAM and copy `TKLCConfigData.<hostname>.sh` file to the newly created vDSR 9.0.X SOAM. After copying the file wait for 5 minutes.

      ```
      cd $FILE_MGMT_AREA


      sudo scp TKLCConfigData.<hostname>.sh admusr@<XMI IP of new vDSR
      9.0.X SOAM VM>:/var/tmp/TKLCConfigData.sh
      ```

   i. SSH to the new vDSR 9.0.X SOAM VM IP and verify the `/var/TKLC/appw/logs/Process/install.log` log file for successfully running of `TKLCConfigData.sh` file. You can run following command to check logs.

      ```
      sudo tail -f /var/TKLC/appw/logs/Process/install.log
      ```

Output:

```
+ sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e04
f2e85fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g/usr/TKLC/
appworks/prod/maint/loaders/install/postInstall/load.AppworksSecConfig
+ /usr/sbin/chpasswd
++ aw.wallet credential get tpdProvd tpdProvd
+ /usr/TKLC/appworks/sbin/updateMylogincnf
Imysql: [Warning] Using a password on the command line interface can
be insecure.
Imysql: [Warning] Using a password on the command line interface can
be insecure.
+ pm.kill apwSoapServer cmsoapa
+ /bin/touch /var/TKLC/appw/TKLCinitcfg
+ /bin/sleep 1
[SUCCESS] script completed successfully!
```

j. Wait for 10 minutes for server to configure with the IP configuration, then reboot the VM using `sudo init 6` command on CLI.

k. Log in to Active DSR NOAM GUI using VIP.

l. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.

m. Select the **SOAM(Level B)** Server group and click **Edit**.

n. Select the new vDSR 9.0.X SOAM VM to add to the SOAM Server group, then click **Ok** to save the changes and wait for 5 minutes.

> **Note:**
>
> After adding new vDSR 9.0.X SOAM VM to SOAM Server group it is configured as Standby SOAM. Post that the newly added vDSR 9.0.X SOAM VM will be considered as Standby SOAM.

o. If the Max Allowed HA Role of the new vDSR 9.0.X SOAM VM is not Active then navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of the new vDSR 9.0.X SOAM VM to Active.

p. ssh to Standby DSR 9.0.X SOAM.

q. Run the following commands to disable the upgrade barrier feature:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

r. Log in to Active vDSR Noam GUI.

s. Navigate to **Status & Manage** from **Main Menu**, then select **Server** and select Standby SOAM and click **Restart**.

6. ssh to Standby 9.0.1 vDSR SOAM and run the following command, if any DSR application (such as PCA, FABR or RBAR) is activated and enabled on DSR.

```
/usr/TKLC/dsr/bin/migrateNonReplicatedData
```

> **Note:**
>
> This step is not required if none of the DSR applications are activated or enabled.

7. To switchover the role of Active SOAM to standby SOAM and standby SOAM to Active SOAM, perform the following steps:
   a. Log in to DSR 9.0.1 Active NOAM VIP.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of Active SOAM HA state to Standby.
8. After switching over, the Standby vDSR 9.0.X VM will be Active and 8.6.X DSR BM NOAM will be Standby.

   Repeat the steps in Migrating BM Standby SOAM to VM to migrate the 8.6.X BM standby SOAM to 9.0.X.

4.3.9 Updating the Database Table Values with vDSR 9.0.1 Value for SOAM

Perform the following procedure to update the database table values with vDSR 9.0.1 value for SOAM.

- Run following command on Active SOAM and Standby SOAM.

```
/usr/TKLC/dsr/bin/updateConfigData 8.6
```

> **Note:**
>
> Ignore the following error while running on Standby SOAM.
>
> `"disallowed write on replicated table"`

4.3.10 Migrating the DAMP Server

Perform the below steps to migrate 8.6.X DAMP BM to 9.0.X VM.

> **Note:**
>
> This procedure can be performed on 20% of DAMPs at once.

1. Remove DAMP from topology.
   a. Log in to Active NOAM DSR GUI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.

c. To change HA state of DAMP to Out of Service (OOS), perform the following steps:
   i. To change DAMP HA state to OOS, perform the following steps:
      i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.
      ii. Click **Edit** and change **Max Allowed HA Role** of DAMP to `OOS`.
   ii. To remove the DAMP instance from DAMP Server group, perform the following steps:
      i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
      ii. Select **DAMP (Level C)** Server Group and click **Edit**.
      iii. Uncheck the required DAMP instance from Server Group and click **OK**.
   iii. Navigate to **Configuration** from **Main Menu**, then select **Servers**. Then, select the DAMP instance which was removed from server group in last step and click **Delete**.

2. Shut down DAMP by running the following command:

   ```
   sudo shutdown -h now
   ```

3. Create vDSR 9.0.1.

   > **Note:**
   > Create DAMP on the same host where NOAM, SOAM VM was created.

4. Assign XMI IP to new vDSR 9.0.1.

   To configure netmask and XMI IP address values, run the following command:

   ```
   sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --netmask=<netmask> --
   device=eth0 --address=<IP address>
   ```

5. Log in to DSR Active vDSR 9.0.1 NOAM using XMI.
6. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
7. Click **Insert**.
8. Add the following details for DAMP server:
   - Enter DAMP hostname
   - Update Role as MP
   - Hardware Profile as DSR Guest
   - Configure XMI and IMI, XSI IP's and NTP server IP
9. Click **Ok**.
10. Select the required DAMP server (which was created in the previous step).
11. Click **Export**, to export server configuration file to the file management folder on the Active NOAM.

12. Now ssh to Active DSR 9.0.X NOAM and copy the `TKLCConfigData.<hostname>.sh` file to the DAMP. After copying the file wait for 5 minutes.

    ```
    cd $FILE_MGMT_AREA


    sudo scp TKLCConfigData.<hostname>.sh admusr@<XMI IP of newly added
    vDSR DAMP>:/var/tmp/TKLCConfigData.sh
    ```

13. ssh to DAMP XMI IP and verify the `/var/TKLC/appw/logs/Process/install.log` log file for successfully running of `TKLCConfigData.sh` file. You can run following command to check logs.

    ```
    sudo tail -f /var/TKLC/appw/logs/Process/install.log
    ```

    Output:

    ```
    + sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
    bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e
    04f2e85fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g/usr/
    TKLC/appworks/prod/maint/loaders/install/postInstall/
    load.AppworksSecConfig
    + /usr/sbin/chpasswd
    ++ aw.wallet credential get tpdProvd tpdProvd
    + /usr/TKLC/appworks/sbin/updateMylogincnf
    Imysql: [Warning] Using a password on the command line interface
    can be insecure.
    Imysql: [Warning] Using a password on the command line interface
    can be insecure.
    + pm.kill apwSoapServer cmsoapa
    + /bin/touch /var/TKLC/appw/TKLCinitcfg
    + /bin/sleep 1
    [SUCCESS] script completed successfully!
    ```

14. Wait for 10 minutes for server to configure with the IP configuration, then reboot the VM using `sudo init 6` command on CLI.
15. Log in to Active vDSR NOAM GUI.
16. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
17. Select the **DAMP (Level C)** Server group and click **Edit**.
18. Select the DAMP instance, which was added while updating DAMP server details, to add to the DAMP Server group. Click **Ok** to save the changes and wait for 5 minutes.
19. If the Max Allowed HA Role of that DAMP instance, which was added to server group in previous step, is not Active then navigate to **Status & Manage** from **Main Menu**. Then, select **HA** and change Max Allowed HA Role of DAMP to Active.
20. ssh to newly added vDSR 9.0.X DAMP.

21. Run the following commands to disable the upgrade barrier feature:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

22. Log in to Active vDSR NOAM GUI.
23. Navigate to **Status & Manage** from **Main Menu**, then select **Server** and select the newly added DAMP instance. Click **Restart**.
24. Run following command on DAMP:

```
/usr/TKLC/dsr/bin/updateConfigData 8.6
```

> **Note:**
>
> - Ignore the following error while running on DAMP error:
>
>   `"disallowed write on replicated table"`
>
> - To configure remaining DAMPs, repeat procedure Migrating the DAMP Server for each 20% of DAMP until you reach 100% of DAMP server.
> - DAMP leader must be migrated last. DC and MP leaders should not be planned in the same migration cycle.

4.3.11 Identifying Standby IPFE Instance

Perform the following procedure to find the Standby IPFE instance.

1. On Active SOAM GUI, navigate to **IPFE** from **Main Menu**, then select **Configuration** and click **Target Sets**.
2. Select the preferred Active IPFE for a Target Set.
   - If IPFE-A1 is mentioned in preferred Active for target set, then IPFE-A2 is standby and vice-versa
   - if IPFE B1 is mentioned in preferred Active for target set, then IPFE-B2 is standby and vice-versa
3. Assume that IPFE-A2 is standby from the above steps.
4. On Active SOAM GUI, navigate to **IPFE** from **Main Menu**, then select **Configuration** and click **Options**.
5. Check which instance IP is mentioned in IPFE-A2 configuration and consider that IPFE instance is Standby IPFE.

4.3.12 Migrating Standby BM IPFE on VM

Perform the following procedure to migrate Standby BM IPFE on VM.

1. Remove Standby IPFE from topology.
   a. Log in to Active NOAM DSR GUI.

b. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.

c. To change HA state of IPFE to Out of Service (OOS), perform the following steps:

   i. To change IPFE HA state to OOS, perform the following steps:

      i. Navigate to **Status & Manage** from **Main Menu**, then select **HA**.

      ii. Click **Edit** and change **Max Allowed HA Role** of IPFE to `OOS`.

   ii. To remove the standby IPFE from IPFE Server group, perform the following steps:

      i. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.

      ii. Select Server Group which contains Standby IPFE instance and click **Edit**.

      iii. Uncheck Standby IPFE instance from Server Group and click **OK**.

   iii. Navigate to **Configuration** from **Main Menu**, then select **Servers** and select Standby IPFE. Click **Delete**.

2. Shutdown IPFE by running the following command:

   ```
   sudo shutdown -h now
   ```

3. Create vDSR 9.0.1.

   > **Note:**
   >
   > Create IPFE on the same host where DAMP, SOAM, NOAM VM was created.

4. Assign XMI IP to new vDSR 9.0.1.

   To configure netmask and XMI IP address values, run the following command:

   ```
   sudo /usr/TKLC/plat/bin/netAdm set --onboot=yes --netmask=<netmask>
   --device=eth0 --address=<IP address>
   ```

5. Log in to DSR Active vDSR 9.0.1 NOAM using XMI.
6. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
7. Click **Insert**.
8. Add the following details for IPFE server:
   - Enter IPFE hostname
   - Update Role as MP
   - Hardware Profile as DSR Guest
   - Configure XMI and IMI, XSI IP's and NTP server IP
9. Click **Ok**.
10. Select the required IPFE server (which was created in the previous step).

11. Click **Export**, to export server configuration file to the file management folder on the Active NOAM.
12. Now ssh to Active DSR 9.0.X NOAM and copy the `TKLCConfigData.<hostname>.sh` file to the IPFE. After copying the file wait for 5 minutes.

    ```
    cd $FILE_MGMT_AREA


    sudo scp TKLCConfigData.<hostname>.sh admusr@<XMI IP of new vDSR IPFE
    instance>:/var/tmp/TKLCConfigData.sh
    ```

13. ssh to IPFE XMI IP and verify the `/var/TKLC/appw/logs/Process/install.log` log file for successfully running of `TKLCConfigData.sh` file. You can run following command to check logs.

    ```
    sudo tail -f /var/TKLC/appw/logs/Process/install.log
    ```

    Output:

    ```
    + sed -i s/WALLET_KEY_TO_BE_REPLACED_DURING_SERVER_EXPORT/
    bc332acff044aa6bcc7871c0742b0b89abd658efc23549acc70d857279a1ee3bb31e04f2e8
    5fcc50fe2fad0c6aa69d3596ecb68f84983b44d7805d98a994ad96/g/usr/TKLC/
    appworks/prod/maint/loaders/install/postInstall/load.AppworksSecConfig
    + /usr/sbin/chpasswd
    ++ aw.wallet credential get tpdProvd tpdProvd
    + /usr/TKLC/appworks/sbin/updateMylogincnf
    Imysql: [Warning] Using a password on the command line interface can be
    insecure.
    Imysql: [Warning] Using a password on the command line interface can be
    insecure.
    + pm.kill apwSoapServer cmsoapa
    + /bin/touch /var/TKLC/appw/TKLCinitcfg
    + /bin/sleep 1
    [SUCCESS] script completed successfully!
    ```

14. Wait for 10 minutes for server to configure with the IP configuration, then reboot the VM using `sudo init 6` command on CLI.
15. Log in to Active vDSR NOAM GUI.
16. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.
17. Select the IPFE (Level C) Server group and click **Edit**.

    > **Note:**
    >
    > Add IPFE to the same server group from where IPFE was removed.

18. Select the newly added vDSR IPFE instance to add to the IPFE Server group, then click **Ok** to save the changes and wait for 5 minutes.
19. If the Max Allowed HA Role of new vDSR IPFE is not Active then navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of that IPFE instance to Active.

20. SSH to newly added vDSR IPFE instance.
21. Run the following commands to disable the upgrade barrier feature:

```
iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
sudo init 6
```

22. Log in to Active vDSR NOAM GUI.
23. Navigate to **Status & Manage** from **Main Menu**, then select **Server** and select **IPFE**. Click **Restart**.
24. Run following command on newly added vDSR IPFE instance:

```
/usr/TKLC/dsr/bin/updateConfigData 8.6
```

> **Note:**
>
> Ignore the following error while running on IPFE error:
>
> `"disallowed write on replicated table"`

4.3.13 Configuring IPFE from SOAM

Perform the following procedure to configure IPFE from SOAM.

- Modify the IPFE options from SOAM.

> **Note:**
>
> These changes are required if IPFE XMI and IMI ip addresses are changed. If IMI and XMI IP addresses are re-used, this step is not required.

1. From Active SOAM GUI, navigate to **IPFE** from **Main Menu**, then select **Configuration** and click **Options**.
2. Configure the IPFE-A1/A2/B1/B2 section, which was considered as Standby.

4.3.14 Switching Over IPFE

Perform the following procedure to switch over IPFE.

1. Add Standby NOAM server in the server group again on DSR 8.6.X Active NOAM, by performing the following steps:
   a. Log in to the VIP of the DSR 8.6.X Active NOAM server.
   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**.
   c. Click **Insert**.

d. Add the following details for NOAM server:
   - Enter NOAM hostname
   - Update Role as Network OAM&P
   - Hardware Profile as DSR Guest
   - Select the NOAM Network element name
   - Configure XMI, IMI IP's, and NTP server IP

e. Click **Ok**.

f. Navigate to **Configuration** from **Main Menu**, then select **Server Groups**.

g. Select the NOAM server group and click **Edit**.

h. Select the standby NOAM to add to the NOAM Server group, then click **Ok** to save the changes. Then, wait for 5 minutes.

2. If the Max Allowed HA role for Standby NOAM is not Active, then navigate to **Status & Manage** from **Main Menu**. Select **HA** and change Standby NOAM Max Allowed HA role to Active by clicking **Edit**.

   a. ssh to vDSR 9.0.1 VM and Run the following commands to disable the upgrade barrier feature:

   ```
   iset -fvalue=1 IdbParamDef where "param='IdbDisableUpgBarrier'"
   sudo init 6
   ```

   b. Log in to Active NOAM GUI.

   c. Navigate to **Status & Manage** from **Main Menu**, then select **Server**, then select Standby NOAM server and click **Restart**.

3. To verify servers, perform the following steps:

   a. Log in to the XMI IP of the vDSR 9.0.1.

   b. Navigate to **Configuration** from **Main Menu**, then select **Servers**. Then, verify if the screen displays data for all the servers in the topology.

   > **Note:**
   >
   > If this verification step fails, do not proceed further. For further help, contact My Oracle Support (MOS).

4. ssh to Standby vDSR 9.0.1 NOAM.

5. Run the following command to check the HA state of the server:

   ```
   ha.mystate -i
   ```

   Output:

   ```
   resourceId      role          node  DC        subResources
   lastUpdate
   ------------------------------------------------------------------------
   ---------------
   ```

```
DbReplication    Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055749.923
VIP              Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055749.925
CacdProcessRes   Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.583
CAPM_HELP_Proc   Act/OOS  BMtoVM-Migtest-DNO01         0
231003:055742.740
DSROAM_Proc      Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.585
CAPM_PSFS_Proc   Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055818.826
VSTPOAM_Proc     Act/Stb  BMtoVM-Migtest-DNO01         0
231003:055948.584
VSTPSERVICE_Proc Act/OOS   BMtoVM-Migtest-DNO01        0
231003:055742.741
```

6. Run the following command, if any DSR application (such as PCA, FABR or RBAR) is activated and enabled on DSR.

   ```
   /usr/TKLC/dsr/bin/migrateNonReplicatedData
   ```

   > **Note:**
   >
   > This step is not required if none of the DSR applications are activated or enabled.

7. To switchover the role of Active NOAM to standby NOAM and standby NOAM to Active NOAM, perform the following steps:
   a. Log in to DSR 8.6.X BM Server using XMI.
   b. Navigate to **Status & Manage** from **Main Menu**, then select **HA** and change Max Allowed HA Role of Active NOAM to Standby.