Oracle® Communications
Performance Intelligence Center
OCPIC 10.4.0 Installation Guide

Release 10.4.0

F26308-05

March 2022

Oracle® Communications Performance Intelligence Center OCPIC 10.4.0 Installation Guide, Release 10.4.0

CAUTION: Use only the guide downloaded from Oracle Help Center.

Table of Contents

MY ORACLE SUPPORT

My Oracle Support (MOS) is your initial point of contact for any of the following requirements:

- **Product Support:**

  The generic product related information and resolution of product related queries.

- **Critical Situations:**

  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.

Training Need:

Oracle University offers training for service providers and enterprises.

A representative at Customer Access Support (CAS) can assist you with MOS registration.

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

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

MOS is available 24 hours a day, 7 days a week.

1. INTRODUCTION

Overview

This document describes the procedures to install “Oracle Communications Performance Intelligence Center” system at Release 10.4.0.

This document is intended for use by trained engineers in software installation on both Oracle and HP hardware. A working-level understanding of Linux, Oracle Database and command line interface is expected to successfully use this document.

It is strongly recommended that prior to performing an installation of the operating system and applications software, the user read through this document.

Related Publications

For information about additional publications that are related to this document, refer to the Release Notice document. The Release Notice document is published as a part of the Release Documentation and is also published as a separate document on the Oracle Help Center.

For security and firewall information refer PIC 10.4 Security Guide of Performance Intelligence Center.

Requirements and Prerequisites

Hardware Requirements

Refer to PIC 10.3 Hardware Guidelines. Of Performance Intelligence Center.

Software Requirements

The following software is required for the release 10.4 installation. The engineers must look on the latest patch available on MOS rather than using the GA release. The recommended patch will be available on MOS Information Center.

Oracle Communication GBU deliverables:

- Management Server
- Mediation Server
- Mediation Protocol
- Acquisition Server
- Acquisition datafeed
- TPD

All the software must be downloaded from Oracle Software Delivery Cloud (OSDC).

https://edelivery.oracle.com/

Reference Documents

[1] Platform Configuration Guide, Tekelec Platform release 7.6

[2] TPD Initial Product Manufacture, Tekelec Platform release 7.6

[3] HP Solutions Firmware Upgrade Pack 2.2.10, Tekelec Platform release 7.6

[4] Oracle Firmware Upgrade Pack, Tekelec Platform release 7.6

[5] Tekelec Default Passwords, CGBU_ENG_24_2229 (restricted access, refer to Appendix E: My Oracle Support)

[6] Hardware Guidelines, F26306-01, Performance Intelligence Center release 10.4.0

[7] Security Guide, F26305-01, Performance Intelligence Center release 10.4.0

[8] Quick Start Guide, F26315-01, Performance Intelligence Center release 10.4.0

[9] Centralized Configuration Manager Administrator Guide, F26318-01, Performance Intelligence Center release 10.4.0

[10] Maintenance Guide, F26312-01, Performance Intelligent Center release 10.4.0

[11] Release Notice, F26302-01, Performance Intelligent Center release 10.4.0

[12] Upgrade Guide, F26309-01, Performance Intelligence Center release 10.4.0

2. INSTALLATION OVERVIEW

This section provides installation overview information by using flowcharts that depict the sequence of procedures for each subsystem and their associated servers.

Note: Each procedure describes a discrete action. It is expected that the individuals responsible for installing the system should reference these flow diagrams during this installation process.

Functional overview

Performance Intelligence Center provides the following main functions:

1) **Management Server:**
   - Can be deployed on Oracle Linux 7.x (latest update 9) based server and can be shared with a Data Record Storage and/or a PDU Storage.
   - Can be deployed on TPD 7.6 only when already installed in a previous release of PIC on TPD.
2) **Data Record Storage:**
   - Can be deployed on Oracle Linux 7.x (latest update 9) based server and can be shared with a Management Server and/or a PDU Storage.
   - Note: Data Record Storage (DRS) in this document can be referenced by its legacy name “DWS” in some command lines.
3) **PDU Storage:**
   - Can be deployed on Oracle Linux 7.x (latest update 9) based server and can be shared with a Management Server and/or a Data Record Storage.
   - Can be deployed on Oracle ZFS engineered system (ZS3-2 and above)
4) **Acquisition and Mediation:**
   - Can be deployed on TPD based server
   - Note: Mediation in this document can be referenced by its legacy name “IXP” in some command lines.
5) **Virtual Machines hosted on the same server**
   - “Management Server, DRS limited to Capacity management, PDU storage, Mediation, Probed Acquisition” Virtual Machines can be hosted on the same server.
   - Multiple integrated acquisition servers can share the same host, but they can’t be hosted along with other components.
   - Each Probed Acquisition Virtual Machine has exclusive usage of its own Acquisition card.

Note: First chapters of this document are describing the installation in a “Bare Metal” environment. Some chapters are dedicated to “Virtual” environment at the end of the document.

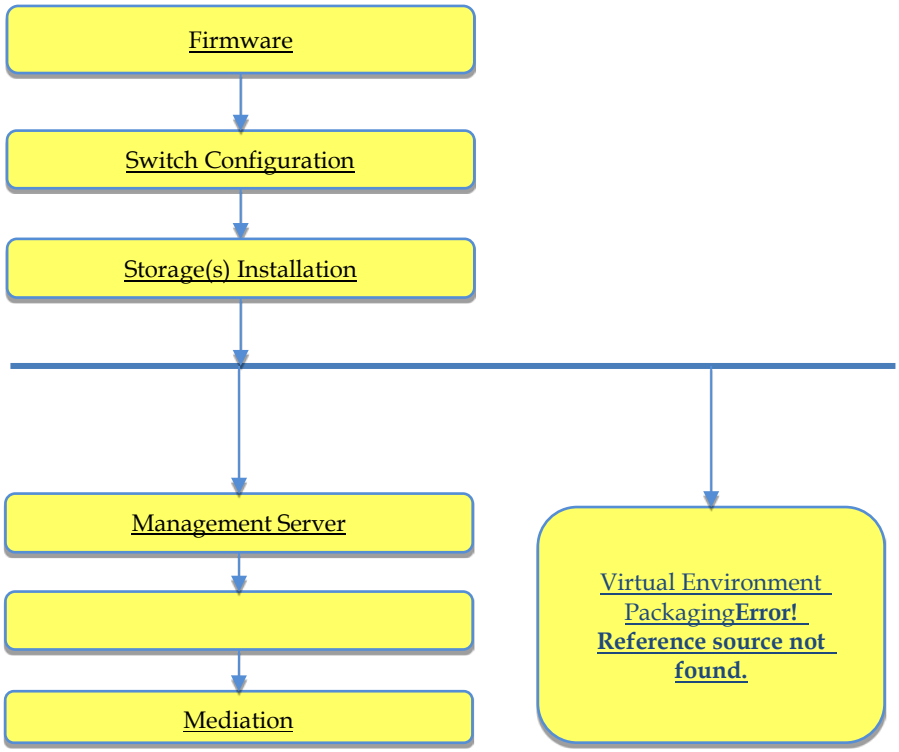
High Level Manufacturing

This flowchart describes high-level manufacturing installation overview.

It is recommended to follow the sequence depicted in below flow chart.

Note: some steps might be done several times because the component is there multiple times.

Figure 1. High level installation



Firmware

Refer to the Oracle Linux installation on RMS server.

Apply the last firmware upgrade, Tekelec Platform release 7.6:

1. HP Solutions Firmware Upgrade Pack 2.2.10
2. Oracle Firmware Upgrade Pack

Switch Configuration

Refer to Hardware Guidelines of Performance Intelligence Center

Storage(s) Installation

Oracle Database(s) Installation

Refer Chapter 6: DWS Installation on Third-Party Server for **Data Warehouse Server (DWS)** Installation on RMS server.

PDU Storage(s) Installation

Refer Chapter 7: PDU Storage Installation on Third Party Server for **Packet Data Unit Storage (PDU)** Installation on RMS server.

Oracle Database(s) and PDU Storage collocated on the same server

The space for each storage is prepared with help of Chapter 4: Oracle Linux Installation on Third Party Server during the Oracle Linux installation on RMS server.

Then each storage is installed accordingly to its own documentation as define above.

Note: Storages must be installed before Mediation Installation

Virtual Environment Packaging

See relevant packaging for your use case:

1. Chapter 12: Virtual Customized Package
2. Chapter 13: Prepackaged DSR Monitoring
3. Chapter 14: Virtual Installation on SUN X7-2
4.

Management Server

Refer to Chapter 8 for Management Server (NSP) Installation on Oracle Linux

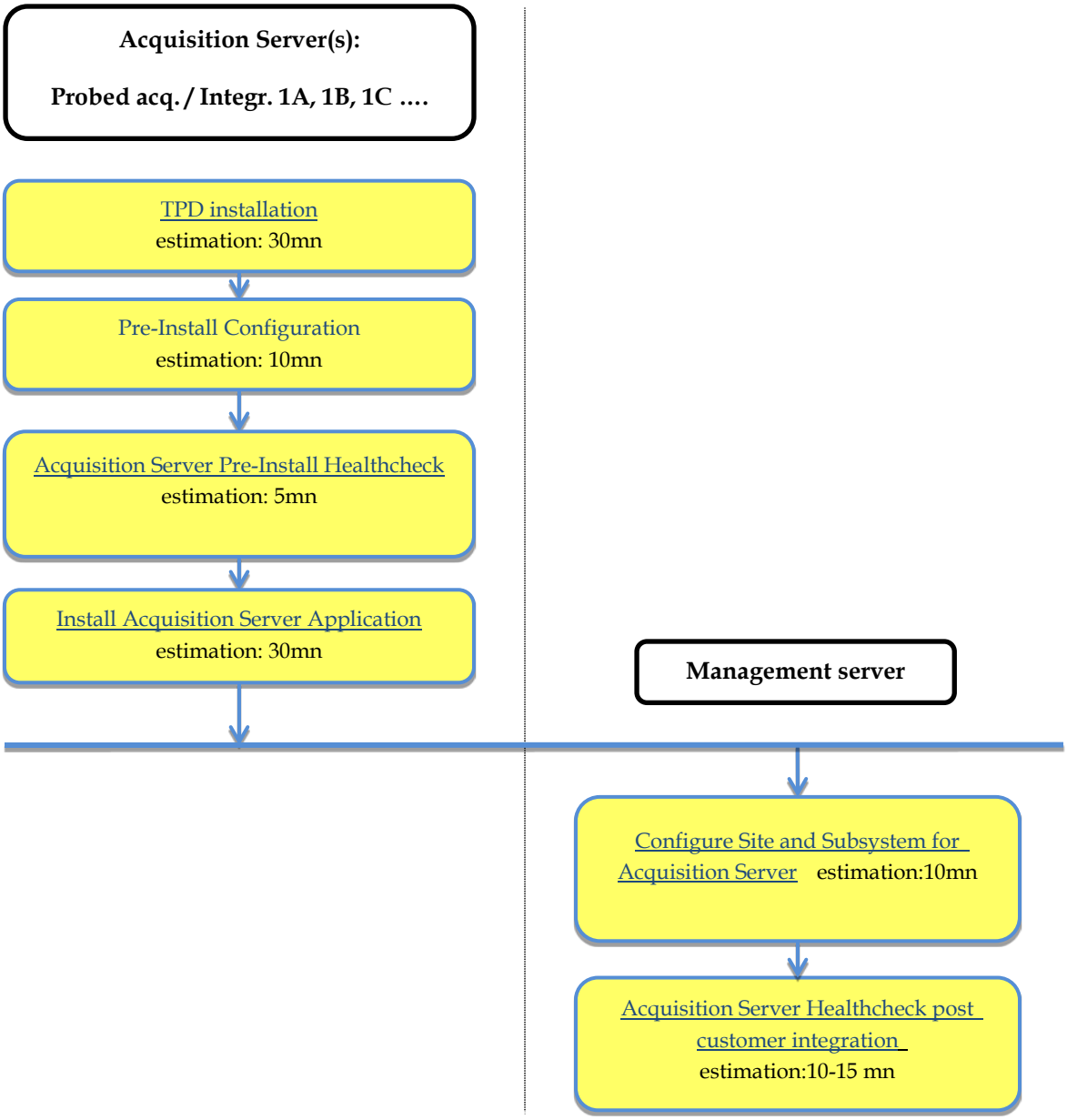
Refer to Chapter 9 for Management Server (NSP) Installation on TPD

Acquisition Subsystem

This flowchart depicts the sequence of procedures that must be executed to install the integrated/probed acquisition subsystem and associated servers.

For Probed acquisition the installation is always done on the stand alone server.

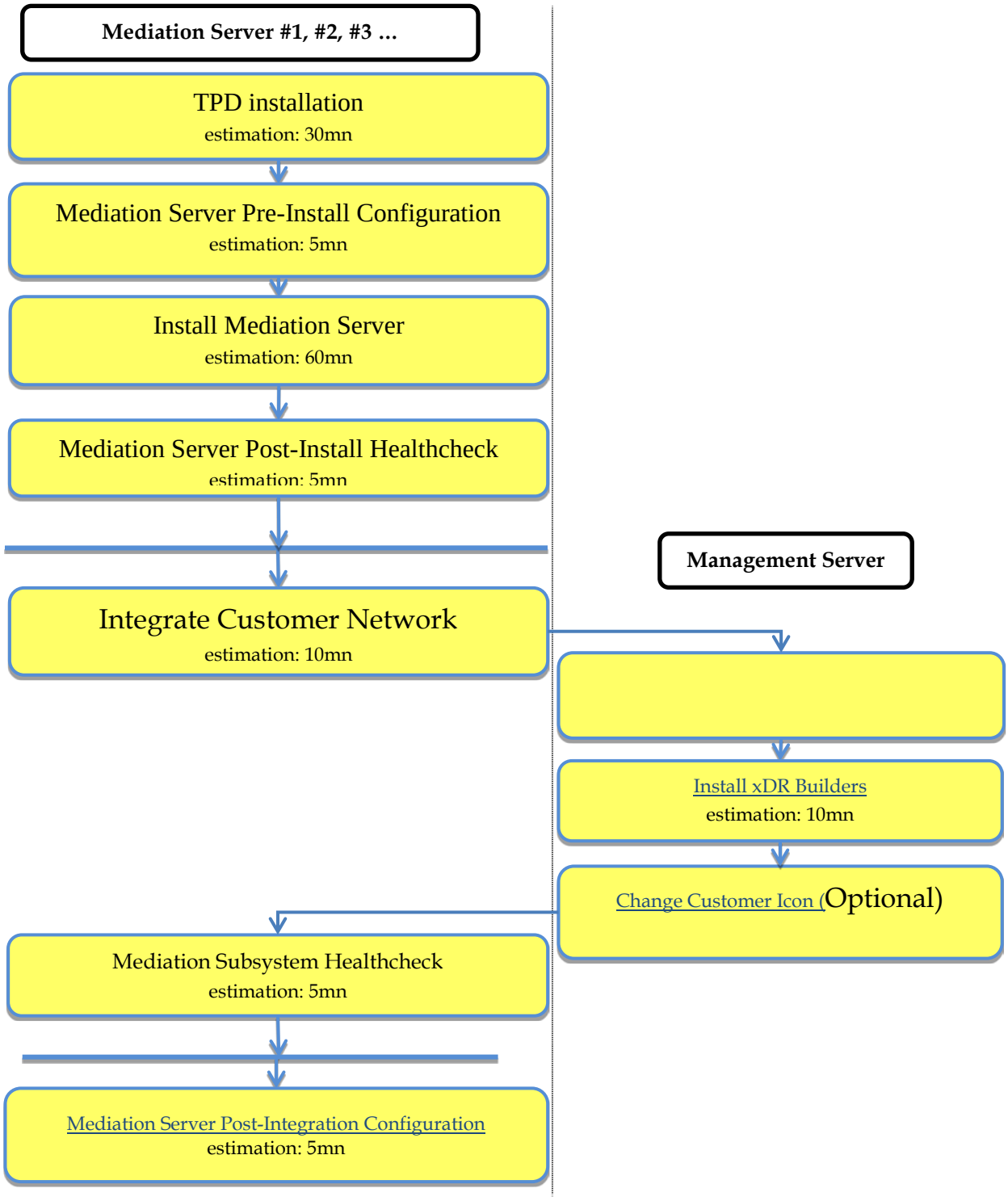
Figure 2. Integrated and Probed Acquisition SubSystem Installation



Mediation Subsystem

This flowchart depicts the sequence of procedures that must be executed to install the mediation subsystem and associated servers. The Mediation subsystem consists of mediation Base server.

Figure 3. Mediation subsystem installation



3. SYSTEM CONFIGURATION ON TPD HARDWARE

This section provides instructions for installing the operating system on the TPD servers, and doing some basic configuration before installing applications.

TPD installation

Follow instructions for OS installation from TPD Initial Product Manufacture of Tekelec Platform

Supported TPD Hardware	Recommended Command	Comments
HP RMS G6, Gen8, Gen9, VM guests	TPDnoraid console=tty0	
X5_2, X6_2,X7-2, VM guests	TPDnoraid console=tty0	
E5-APP-B	TPDlvm	This command is to be used for a fresh installation on a new hardware, never used before for any purpose.
	TPDlvm scrub	Use this command for a major upgrade and when there was an application already installed.

Table 1: TPD and HW supported for Performance Intelligence Center 10.4.0

Caution: No JRE is delivered anymore. It has to be installed after the application. Refer to the mediation and acquisition subsystem installation steps.

4. ORACLE LINUX INSTALLATION ON THIRD PARTY SERVER

Purpose

This page explains how to install Oracle Linux 7.x on a third-party servers in preparation of Performance Intelligence Center (PIC) product installation.

Prepare for Installation

We recommend to use edelivery: https://edelivery.oracle.com/linux to download the latest release of Oracle Linux 7 (7.9) for x86_64 bit systems.

The section below is described using HP DL380 Gen9 server.

To install the server you will need a console access, we recommend using iLO access it also allows you to mount ISOs images. To access the iLO remotely a IP address must be assigned to it, Refer to "HP UEFI System Utilities User Guide for HP ProLiant Gen9" if you don't know how to configure it.

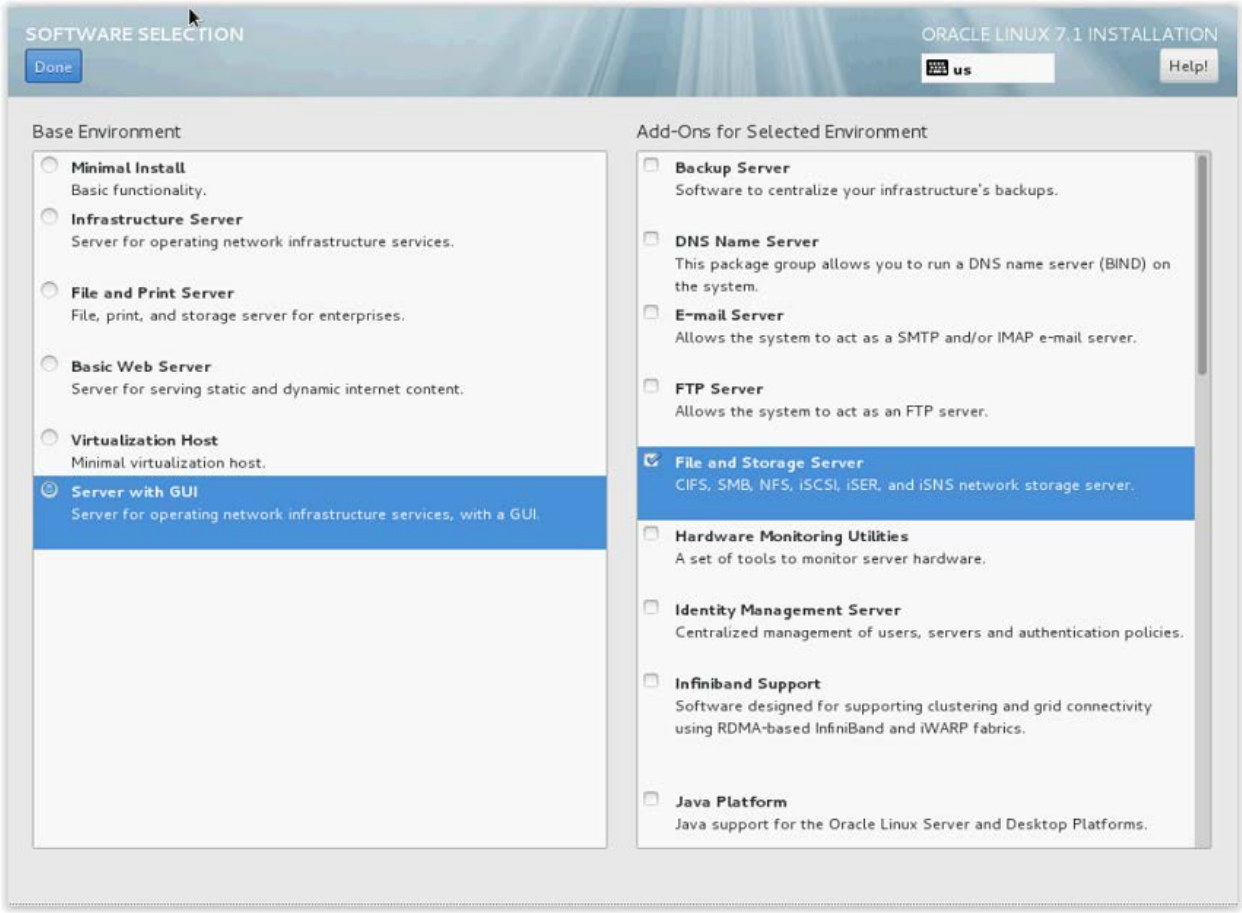
The HP Smart Array P440ar RAID controller must be configured to support the installation of Oracle Linux and the ASM diskgroup, alternatively the RAID array can be used to store PDUs. Please follow "HP Smart Storage Administrator User Guide" if you don't know how to configure it. The recommended configuration is the following (refer to Hardware installation guideline for details):

- One RAID 1 logical drive built with the two hard drives in order to host Oracle Linux installation.
- For Mediation server: a RAID 10 logical drive built with 24 hard drives can be used, that configuration provides higher bandwidth but lower storage capacity. Alternatively a six RAID 5 logical drives built with four hard drives each to host the 6 ASM diskgroup can be used, that configuration provides lower bandwidth but slightly higher storage capacity
- For Management server: a RAID 10 logical drive built with 4 hard drives can be used for Oracle ASM/Database storage. In order to store the daily backup, an optional logical drive created from 2 hard drives in RAID 1 can be created.
- For Packet Data Unit (PDU) server: a RAID 10 logical drive built with 24 hard drives to store the PDUs generated by the Mediation servers.
- For Prepackaged DSR monitoring: a RAID 10 logical drive built with 6 hard drives to store the PDUs generated by the Mediation servers.

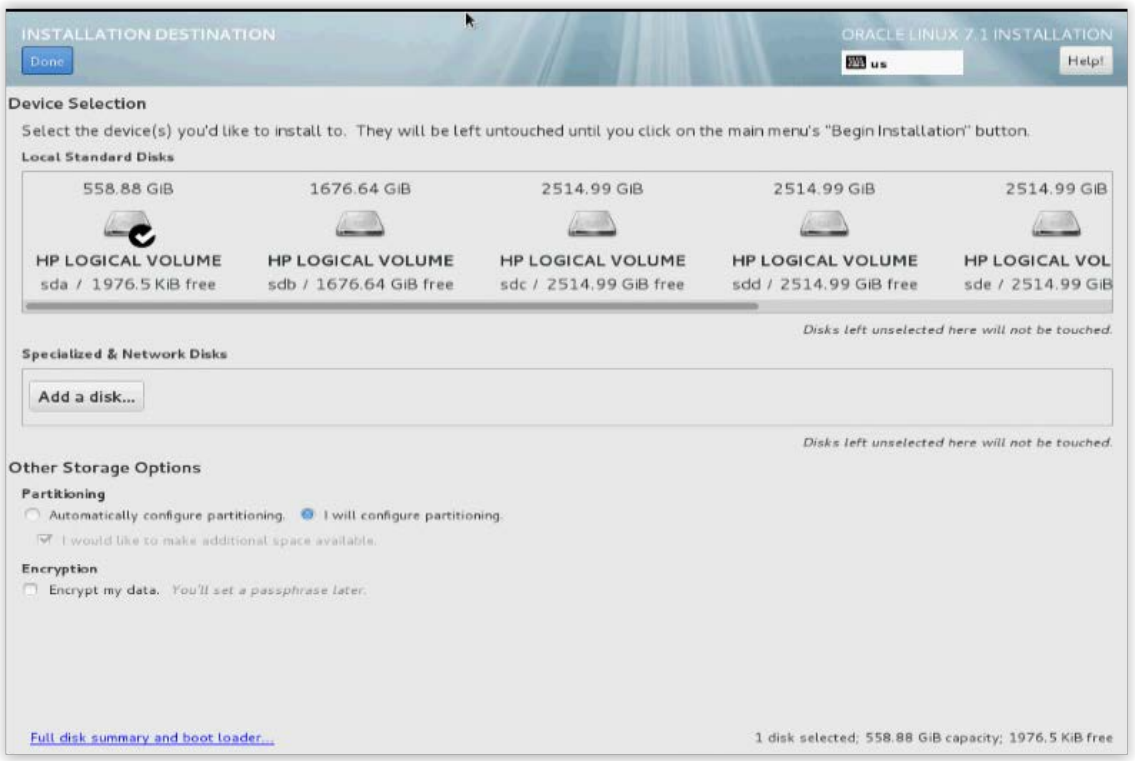
Install Oracle Linux7

Note: Screen capture used in the section are from previous OL version

1. Refer to "Oracle Linux 7 Installation Guide" documentation to install Oracle Linux. Boot the server on using OL iso image to start the installation. Default language during the installation will be set to English (en).
2. Follow Chapter 2 "Installing Oracle Linux Manually":
    1. Section 2.1.3 choose Base environment "Server with GUI" and Add-Ons "File and Storage Server". If the server is intended to be used as KVM hypervisor, select also Add-Ons "Virtualization Client", “Virtualization Hypervisor” and "Virtualization Tools”.



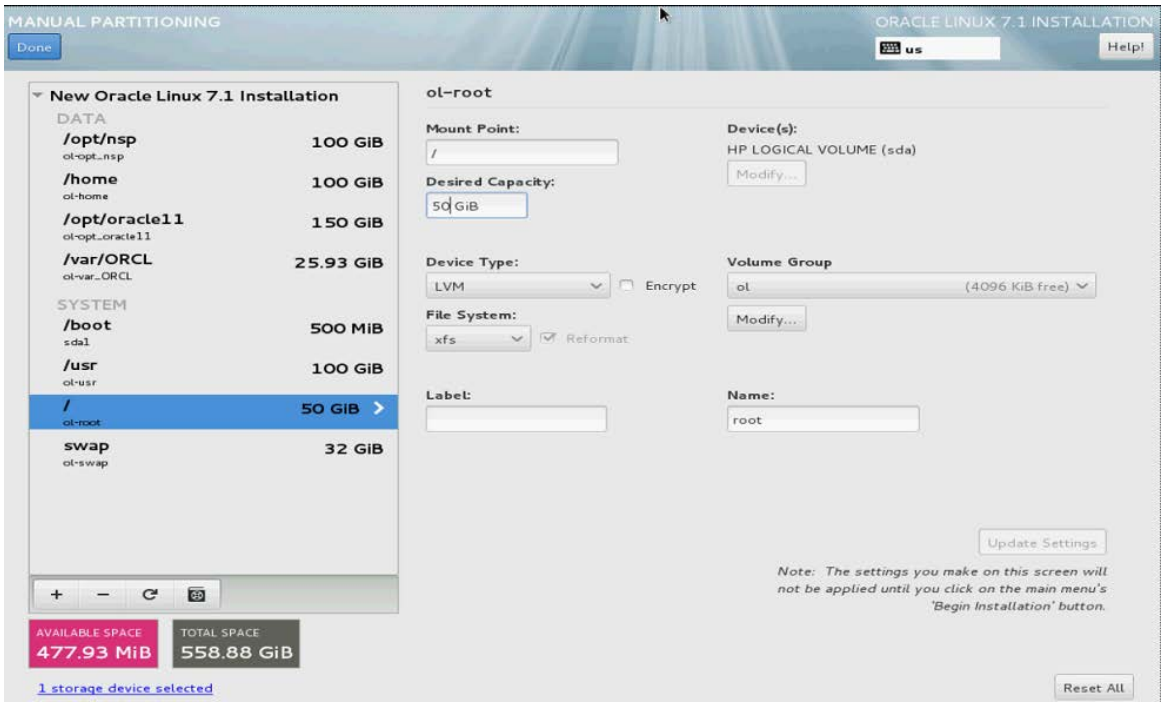
2. Section 2.1.4 you need the select the "Installation Destination", as explained before Oracle Linux 7.x is going to be installed on a RAID 10 logical drive built with the two 900GB drives



3. Select "I will configure partitioning" and click on "Done" button, a new configuration window will be displayed:

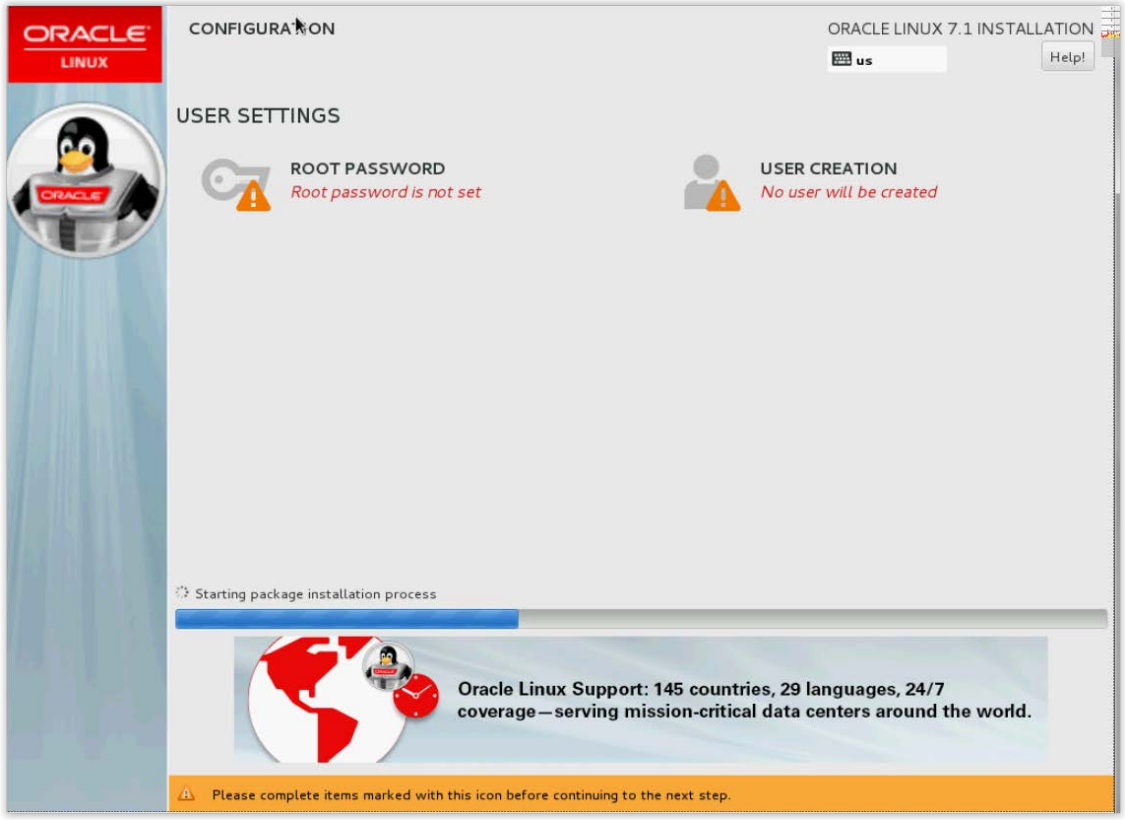
NOTE: If you are installing Oracle 19c replace /opt/oracle11 by /u01/app

Refer to System Partitioning Recommendation **Appendix D: System Partitioning Recommendation**, in order to define the partitions and their size.



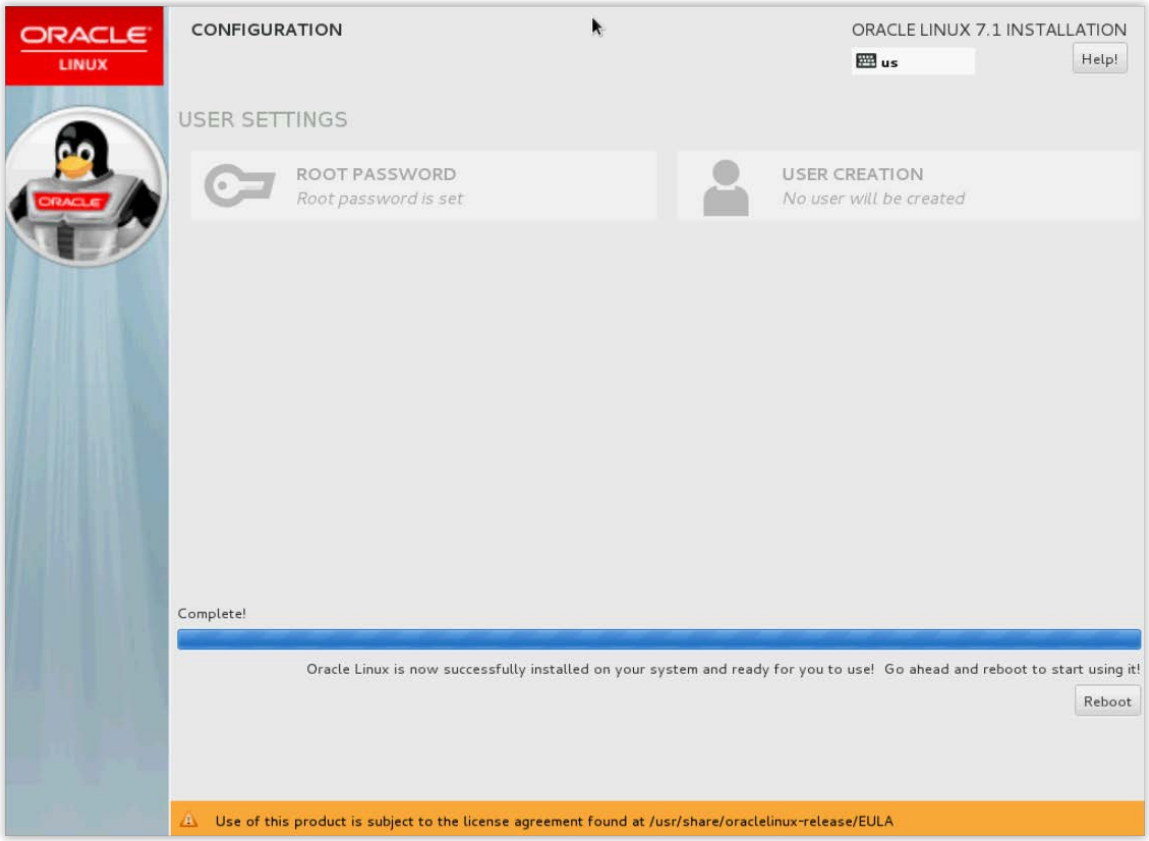
4. Shrink /home logical volume to 100GB, adjust the SWAP size to match the amount of RAM installed on your server and create a new logical volumes called /opt/oracle11 (150GB again name that partition /u01/app if installing Oracle 19c), /opt/nsp (100GB only if you plan to install MGMT software) and /var/ORCL (remaining space available) . Click on "Done" button (If some Logical volumes had been previously created the wizard will ask you to confirm changes, please click on "Delete All" and then "Reclaim Space".
   Note that the size of each partition can be adjusted depending on the size of the RAID ARRAY.
5. Click "Network & Hostname" option on the Installation Summary screen to configure the network connection, adjust the configuration to the customer network (IP/Mask/Gateway) and enable the interface.
6. Once you have selected all your installation configuration options, click Begin Installation on the Installation Summary screen to start the installation.

7. The installation begins and the wizard gives you the option to configure root password:

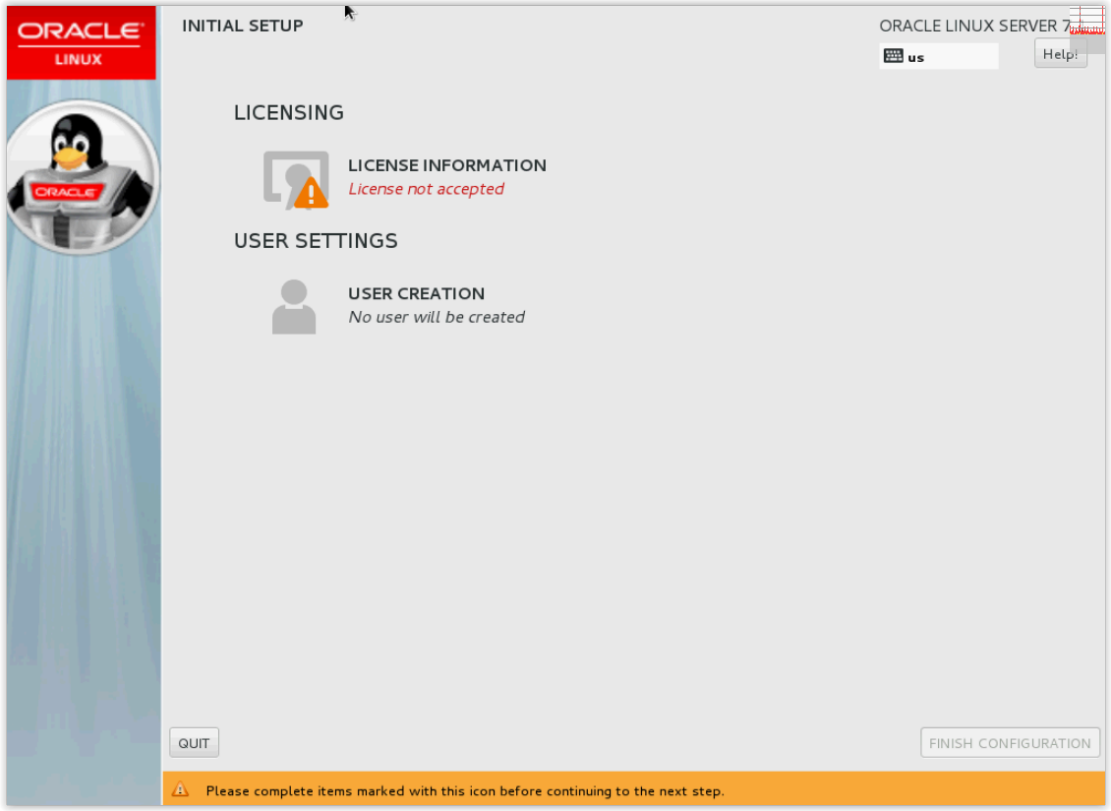


8. Choose the root password and click on "Done" button, you are given the option to create other users: you can create the standard admusr user if you want to but not cfguser.

9. Wait until the installation completes, the wizard will then ask you to reboot: click on "Reboot"



10. During the reboot you will have to accept the License Information:



11. Accept the License information and click on finish configuration. You will be asked to install software update, as you will most likely not have internet access choose not to.

Configure Server Prior to Oracle ASM and Database Install

1. Use a ssh client to access the server via the IP you configured during Oracle Linux installation.
2. Log as root and edit /etc/hosts to add an entry with the server IP and hostname, for example (only one IP address/hostname per line):

```
10.20.30.40     OLGen9DWS
```

3. Configure Oracle Linux firewall to accept external connection to Oracle database:

```
# firewall-cmd --permanent --add-port=1158/tcp
# firewall-cmd --permanent --add-port=1521/tcp
# firewall-cmd --permanent --add-port=443/tcp
# firewall-cmd --permanent --add-port=80/tcp
# firewall-cmd --permanent --add-port=49696/tcp
# firewall-cmd --permanent --add-port=1099/tcp
# firewall-cmd --permanent --add-port=7051/udp
# firewall-cmd --permanent --add-port=8001/tcp
# firewall-cmd --permanent --add-port=7001/tcp
# firewall-cmd --permanent --add-port=7003/tcp
# firewall-cmd --permanent --add-port=5556/tcp
# firewall-cmd --permanent --add-port=41090/tcp
```

```
# firewall-cmd --permanent --add-port=41000/tcp
# firewall-cmd --reload
```

4. Disable SELINUX: edit /etc/sysconfig/selinux and change the following line "SELINUX=enforcing" to "SELINUX=disabled", save and exit.

5. Add tmpfs to /etc/fstab: use vi to edit /etc/fstab and add the following line (**adjust the size** based on the amount of memory you want to assign to Oracle DB):

```
tmpfs                   /dev/shm                tmpfs   size=32G      0 0
```

6. Mount /dev/shm:

```
# mount -o remount /dev/shm
```

7. Reboot the server

Configure Local Yum repository from Oracle Linux ISO

1. Copy Oracle Linux iso image to /var/ORCL
2. Create a new mount point called /mnt/repository

```
# mkdir -pv /mnt/repository
```

3. Mount Oracle Linux iso image

```
# mount -o loop /var/ORCL/V*.iso /mnt/repository
```

4. Copy the attached file local.repo to /etc/yum.repos.d/

local.repo

5. Run the following commands to add yum repository

```
# yum clean all
# yum-config-manager --disable ol7_UEKR3 (if Oracle Linux release 7.1 or 7.2)
# yum-config-manager --disable ol7_UEKR4 (if Oracle Linux release 7.3 or more)
```

```
# yum-config-manager --disable ol7_UEKR5 (if Oracle Linux release 7.7)
# yum-config-manager --disable ol7_UEKR6 (if Oracle Linux release 7.9)

# yum-config-manager --disable ol7_latest
# yum repolist
```

Configure NTP service for time synchronization

1. As **root** user install ntp package:

```
# yum install ntp
```

2. Copy the attached ntp.conf to /etc (overwrite the existing one)


ntp.conf

3. Edit /etc/hosts and add the ntp source IP provided by the network administrator (example is for a NTP IP = 10.20.30.40):

10.20.30.40 ntpserver1

4. Enable and restart ntpd service:

```
# systemctl enable ntpd
# systemctl disable chronyd
# systemctl restart ntpd
```

The provided NTP configuration allows the NSP server to sync with a NTP source but it does not allow the NSP server to act as an NTP source.

If you wish to use the NSP server as an NTP source run the following steps as **root** user (these steps are **OPTIONAL**, execute them only to use NSP as NTP source):

1. Open UDP port 123:

```
#firewall-cmd --permanent --add-port=123/udp;firewall-cmd --reload
```

2. Edit /etc/ntp.conf and replace 127.0.0.1 with the back end IP of the NSP.
3. Restart ntp service:

```
#systemctl restart ntpd
```

Configure Front End Interface for Management Server

In order to separate the http interface (front end) from the other servers (back end) we configure two interfaces on the MGMT (NSP) server.

During the Oracle Linux installation, one of these interface has been configured, this is the back end interface that is used to connect all the servers used in the PIC system.

To provide http access via another interface, you must configure a second ethernet interface, for example eno2: edit /etc/sysconfig/network-scripts/ifcfg-eno2 to provide the IP address and subnet for the front end interface.

As the newly configured interface is part of another subnet you need to configure a static route for that interface in order to route the http request to the proper gateway. In the example of eno2 interface create a file called /etc/sysconfig/network-scripts/route-eno2 containing the following:

```
ADDRESS0=X.X.X.X
NETMASK0=X.X.X.X
GATEWAY0=X.X.X.X
```

where ADDRESS0=X.X.X.X is the network number for the static route.

NETMASK0=X.X.X.X is the netmask for the network number defined with ADDRESS0=X.X.X.X.

GATEWAY0=X.X.X.X is the default gateway, or an IP address that can be used to reach ADDRESS0=X.X.X.X

5. ORACLE 19C ASM AND DATABASE INSTALLATION ON THIRD PARTY SERVER

Purpose

This chapter explains how to install a Oracle 19c ASM and Database software on a third-party server.

This chapter is applicable for a server with Oracle Linux installed by following the procédure from chapter 4 Oracle Linux Installation on Third Party Server.

Scope

The software version used for this document is Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 – (Production Version 19.3.0.0.0) 64bit installed on an Oracle Linux 7.x (latest update 9) server.

This guide is based on a HP DL380 Gen 9 server configuration. The recommended hardware configuration description can be found in PIC 10.4.0 Hardware Installation Guideline

Prepare for Installation

- The following KM will help you find the latest Oracle 19c release available "Release Schedule of Current Database Releases" (Doc ID 742060.1). This guide is based on Linux x86_64 Oracle 19c software (V982068-01.zip, V982063-01.zip) which can be downloaded from Oracle Software Delivery Cloud.
- Download Oracle asmlib from oracle download: http://www.oracle.com/technetwork/server-storage/linux/asmlib/ol7-2352094.html

Configure Server prior to Oracle ASM and Database Installation

1. As root user, create groups and user for Oracle installation:

```
# groupadd oinstall;useradd -d /home/oracle -g oinstall oracle;passwd oracle

(Enter a password of your choice for oracle user)


# useradd -d /home/grid -g oinstall grid;passwd grid

(Enter a password of your choice for grid user)


# groupadd asmadmin;groupadd asmdba;groupadd asmoper;groupadd oper;groupadd dba;groupadd bckpdba;groupadd dgdba;groupadd kmdba;groupadd racdba
# usermod -a -G asmdba oracle
# usermod -a -G asmdba grid
# usermod -a -G asmoper grid
# usermod -a -G asmoper oracle
# usermod -a -G oper oracle
# usermod -a -G asmadmin grid
# usermod -a -G dba grid
# usermod -a -G dba oracle
# usermod -a -G asmadmin oracle
# usermod -a -G bckpdba oracle
```

```
# usermod -a -G dgdba oracle
# usermod -a -G kmdba oracle
# usermod -a -G racdba oracle
```

2. Change owner of /u01/app and create default folders:

```
# chown -R oracle:oinstall /u01/app;chmod 775 /u01/app
# mkdir -pv /u01/app/grid
# mkdir -pv /u01/app/grid/product/19.3.0/grid
# chown -R oracle:oinstall /u01/app/grid
# mkdir -pv /u01/app/oracle
# mkdir -pv /u01/app/oracle/product/19.3.0/dbhome_1
# chown -R oracle:oinstall /u01/app/oracle
# mkdir -pv /u01/app/oraInventory
# chown oracle:oinstall /u01/app/oraInventory
# chmod 770 /u01/app/oraInventory
```

3. Edit /home/grid/.bash_profile and add the following lines:

```
export ORACLE_BASE=/u01/app/grid
export ORACLE_HOME=/u01/app/grid/product/19.3.0/grid
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
export PATH=$ORACLE_HOME/bin:$PATH
export ORACLE_SID="+ASM"
export LISTENER_NAME="LISTENERASM"
export ORAENV_ASK=NO
```

4. Edit /home/oracle/.bash_profile and add the following lines:

```
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/oracle/product/19.3.0/dbhome_1
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
export PATH=$ORACLE_HOME/bin:$PATH
export ORAENV_ASK=NO
```

5. Edit /etc/security/limits.conf and add the following lines:

```
oracle soft nofile 4096
oracle hard nofile 65536
oracle soft stack 10240
grid soft nofile 4096
grid hard nofile 65536
grid soft stack 10240
```

6. Install oracle-rdbms-server-12cR1-preinstall, oracleasm-support and oracleasmlib on the server using the local yum repository.

```
# mount -o loop /var/ORCL/V*.iso /mnt/repository
```

For OL 7.6 or prior, execute:

```
# yum install oracle-database-server-12cR2-preinstall.x86_64

# yum install oracleasm-support
```

Or

For OL 7.7 or above, execute:
yum install oracle-database-preinstall-19c.x86_64

yum install oracleasm-support

7. Copy Oracle asm lib rpm package to /var/ORCL and install it:

```
# rpm -ivh /var/ORCL/oracleasmlib-*.x86_64.rpm
```

Install and Configure ASM

1. As **root** user, configure oracleasm for grid user:

```
# /usr/sbin/oracleasm configure -i
Default user to own the driver interface []: oracle
Default group to own the driver interface []: oinstall
Start Oracle ASM library driver on boot (y/n) [ n ]: y
Scan for Oracle ASM disks on boot (y/n) [y]: y
```

2. Reboot the server
3. The recommended configuration is RAID 1, the disk Array has been created during the installation of Oracle Linux Prepare the server for installation) :
   Create partitions and ASM disks:
   1.
      i. Use parted to create one partition based on the RAID 1 logical drive built during Oracle Linux installation. The example is for a 10TB logical drive called /dev/sdb , these commands will create a 10TB partition named /dev/sdb1:

      You can list the current partitions with **parted /dev/sda print list,all**

      ```
      # parted /dev/sdb mklabel gpt
      # parted /dev/sdb mkpart primary 0GB 10TB
      ```

      ii. Create ASM disks with the following commands:

      ```
      # /usr/sbin/oracleasm createdisk asm0 /dev/sdb1
      ```

Note: the zip file name can be different for the given installation, the user is expected to update the command with the correct name.

4. Copy the V982068-01.zip to /var/ORCL and change the ownership to **oracle** user:

```
# chown oracle:oinstall /var/ORCL/V982068-01.zip
```

5. As **oracle** user unzip V982068-01.zip file to /u01/app/grid/product/19.3.0/grid folder.

```
# cd /u01/app/grid/product/19.3.0/grid

# unzip /var/ORCL/V982068-01.zip
```

6. You'll now have to start the ASM installation using silent install with a response file. Use the ASM response file attached (**ASMsetup193c.rsp**) to this document and customize it to match your configuration. The usual customization are the following lines:

ASMsetup193c.rsp

   i. oracle.install.asm.SYSASMPassword= **enter the password you chose for SYSASM user (must be 8 characters with 1 capital and 1 special character)**
   ii. oracle.install.asm.monitorPassword= **enter the password you chose for MONITOR user (must be 8 characters with 1 capital and 1 special character)**
   iii. oracle.install.asm.diskGroup.disks=/dev/oracleasm/disks/ASM0 **declare the ASM disks created at step 3 ii.**

7. Once you have customized and copied the response file the server (for example in /home/oracle) start the ASM installation with the following command :

```
# cd /u01/app/grid/product/19.3.0/grid
# ./gridSetup.sh -silent -force -responseFile /home/oracle/ASMsetup193c.rsp
```

8. Wait until the installation completes and displays the following message :

```
Successfully Setup Software.
```

9. As **root** user run the following command:

```
# /u01/app/oraInventory/orainstRoot.sh
```

10. As **root** user, execute the last step to finish ASM install

```
# /u01/app/grid/product/19.3.0/grid/root.sh
```

11. As **oracle** user, complete the configuration by executing the following command:

```
#/u01/app/grid/product/19.3.0/grid/gridSetup.sh -executeConfigTools -responseFile /home/oracle/ASMsetup193c.rsp -silent
```

Install and Configure Oracle Database

1. Copy the V982063-01.zip to /var/ORCL and change the ownership to **oracle** user

```
# chown oracle:oinstall /var/ORCL/V982063-01.zip
```

2. As **oracle** user unzip V982063-01.zip file to /u01/app/oracle/product/19.3.0/dbhome_1 folder:

```
#cd /u01/app/oracle/product/19.3.0/dbhome_1

#unzip /var/ORCL/V982063-01.zip
```

3. Start the Database installation with runInstaller, do it step by step with the GUI version from an X server session or run a silent install with a response file. If you choose to use a response file please use the one listed in the attachments (DBsetup193c.rsp)

DBsetup193c.rsp

Note:

4. Once you have customized and copied the response file the server (for example in /home/oracle) start the Database installation with the following command as oracle user:

```
# cd /u01/app/oracle/product/19.3.0/dbhome_1
# ./runInstaller -silent -force -responseFile /home/oracle/DBsetup193c.rsp
```

5. Wait until the installation completes and displays the following message :

```
"Successfully Setup Software."
```

6. As **root** user, run the following command:

```
# /u01/app/oracle/product/19.3.0/dbhome_1/root.sh
```

7. As **grid** user, verify ASM is properly installed and started with the following crsctl command:

```
# crsctl status resource -t
```

The expected output is the following:

```
--------------------------------------------------------------------------------
Name Target State Server State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.DATA.dg
               ONLINE ONLINE ol19ctest STABLE
ora.LISTENER.lsnr
               ONLINE ONLINE ol19ctest STABLE
ora.asm
               ONLINE ONLINE ol19ctest Started,STABLE
ora.ons
               OFFLINE OFFLINE ol19ctest STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.cssd
      1        ONLINE ONLINE ol19ctest STABLE
ora.diskmon
      1        OFFLINE OFFLINE STABLE
ora.evmd
      1        ONLINE ONLINE ol19ctest STABLE
--------------------------------------------------------------------------------
```

Linux, ASM and Database binaries are now properly installed. The next steps consists in:

- installing the PIC DWS Schema DWS Installation on Third-Party Server
  OR
- Management Server (NSP) 10.4.0 Management Server (NSP) Installation on Third-Party Server

6. DWS INSTALLATION ON THIRD-PARTY SERVER

Purpose

This chapter explains how to install the oracle instance and schema mandatory for to build a Mediation Storage Server (DWS) on a third-party server with Oracle Linux.

This chapter can be applied on a server with Oracle Linux installed after performing procedures mentioned in chapter Oracle Linux Installation on Third Party Server and Oracle 19c ASM and Database Installation on Third Party Server.

Prepare for Installation

We recommend to use edelivery: https://edelivery.oracle.com/ to download Oracle Performance Intelligence Center MEDSRV 10.4.0 or use the latest patch available on MOS 1989320.2

Create IXP Database and deploy IXP Schema

1. As **root** user update /home/oracle/.bash_profile and add the following lines:

```
export ORACLE_SID="IXP"
export ORACLE_INST="IXP"
export ORACLE_UNQNAME="IXP"
```

If you have already installed Management Server (NSP) application on this server then DO NOT add these lines in /home/oracle/.bash_profile. Just type in the same commands in a shell as oracle user (make sure you do so every time you open a new shell as oracle during this procedure).

2. As **oracle** user load oracle environment:

```
# export ORACLE_SID="IXP"
# export ORACLE_INST="IXP"
# export ORACLE_UNQNAME="IXP"
```

3. Create default directory for IXP database:

```
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/adump
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/pfile
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/cdump
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/bdump
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/udump
# mkdir -pv $ORACLE_BASE/oradata/$ORACLE_SID/flash_recovery_area
# mkdir -pv $ORACLE_BASE/redo/$ORACLE_SID
# mkdir -pv $ORACLE_BASE/oraindex/$ORACLE_SID
# mkdir -pv $ORACLE_BASE/logs
```

4. Create Oracle password file. Customize the password to match security requirements (at least 8 letters, symbols, ...):

```
# orapwd force=y file=$ORACLE_HOME/dbs/orapw$ORACLE_SID password=Tekelec1$
```

5. Copy the oracle init file to the server:
   a. If you are installing Oracle 11g copy the attached initIXP11g.ora file to /opt/oracle11/oracle/product/11.2.0/dbhome_1/dbs/
   b. if you are installing Oracle 12c copy the initIXP12c.ora to /u01/app/oracle/product/12.1.0/dbhome_1/dbs/
   c. if you are installing Oracle 19c copy the initIXP12c.ora to /u01/app/oracle/product/19.3.0/dbhome_1/dbs/

Edit the init file and customize the "**memory_target=**" parameter depending on the amount of physical memory available on you server: for example use **24GB** on a server containing **32GB** of physical RAM, Refer to Oracle Data Administrator Guide for details.
2062990.1 contains one example for memory target, processes and open_cursors.

6. Rename oracle init file:
   a. If installing Oracle11g:


```
cp /opt/oracle11/oracle/product/11.2.0/dbhome_1/dbs/initIXP11g.ora/opt/oracle11/oracle/product/11.2.0/dbhome_1/dbs/initIXP.ora
```

   b. If installing Oracle 12c (12.**1**):


```
cp /u01/app/oracle/product/12.1.0/dbhome_1/dbs/initIXP12c.ora/u01/app/oracle/product/12.1.0/dbhome_1/dbs/initIXP.ora
```

   c. if installing Oracle 12c (12.**2**):


```
cp /u01/app/oracle/product/12.2.0/dbhome_1/dbs/initIXP122c.ora/u01/app/oracle/product/12.2.0/dbhome_1/dbs/initIXP.ora
```

   d. if installing Oracle 19c (19.**3**):


```
cp /u01/app/oracle/product/19.3.0/dbhome_1/dbs/ initIXP.ora /u01/app/oracle/product/19.3.0/dbhome_1/dbs/initIXP.ora
```

7. Connect to sqlplus:

```
# sqlplus / as sysdba
```

8. Startup the database in NOMOUNT:

```
# startup NOMOUNT
```

9. Create Database IXP:

```
CREATE DATABASE IXP
    CONTROLFILE REUSE
    LOGFILE GROUP 1 ('+DATA') SIZE 20G,
        GROUP 2 ('+DATA') SIZE 20G,
        GROUP 3 ('+DATA') SIZE 20G,
        GROUP 4 ('+DATA') SIZE 20G
    DATAFILE '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G,
        '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G
        EXTENT MANAGEMENT LOCAL
    SYSAUX DATAFILE '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G,
        '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G
    DEFAULT TEMPORARY TABLESPACE temp
        TEMPFILE '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G
            EXTENT MANAGEMENT LOCAL UNIFORM SIZE 10M
    UNDO TABLESPACE undo
        DATAFILE '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G,
            '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 32G
    CHARACTER SET AL32UTF8
    SET TIME_ZONE = 'America/New_York';
```

10. Execute sql scripts:

```
@$ORACLE_HOME/rdbms/admin/catalog.sql
@$ORACLE_HOME/rdbms/admin/catblock.sql
@$ORACLE_HOME/rdbms/admin/catproc.sql
@$ORACLE_HOME/rdbms/admin/dbmspool.sql
exit
```

11. Set the ‘system’ user password.

```
# sqlplus / as sysdba
```

```
alter user system identified by system_user_password;                <<replace system_user_password with password>>

exit
```

12. Exit sqlplus and log as system user:

```
# sqlplus system/******      <<replace ****** by system user password>>

@$ORACLE_HOME/sqlplus/admin/pupbld.sql
exit
```

13. Wait 2 minutes and verify that listener is seeing IXP and ASM instances:

```
# lsnrctl status
```

Expected output:

```
Service "+ASM" has 1 instance(s).
  Instance "+ASM", status READY, has 1 handler(s) for this service...
Service "IXP" has 1 instance(s).
  Instance "IXP", status READY, has 1 handler(s) for this service...
The command completed successfully
```

14. Create spfile:

```
# sqlplus / as sysdba
shutdown immediate

create spfile from pfile;
startup mount
alter database open;
alter system register;
shutdown immediate
exit
```

15. Register Oracle database with has:

```
# srvctl add database -d $ORACLE_SID -o $ORACLE_HOME -n $ORACLE_SID -a "DATA"
```

16. Start Oracle database with has:

```
# srvctl start database -d $ORACLE_SID -o OPEN
```

17. As **root** user mount PIC MEDSRV iso image and copy the content of the migration directory, change permissions to 777 to this directory and its subfolder.

```
# mkdir -p /mnt/upgrade
```

Copy the PIC MEDSRV ISO in /var/ORCL directory and mount it to /mnt/upgrade

```
# mount -o loop /var/ORCL/PIC-MEDSRV-10.*0-x86_64.iso /mnt/upgrade
```

Copy the content of the migration directory and change its permission including all the sub-directories

```
# cp -r /mnt/upgrade/migration /home/oracle
# mkdir -p /home/oracle/migration/oracle/utils/trc
# mkdir -p /home/oracle/migration/oracle/tuning/trc
# mkdir -p /home/oracle/migration/oracle/schema/trc
# mkdir -p /home/oracle/migration/oracle/instance/trc
# chown -R oracle:oinstall /home/oracle/migration
# chmod 777 -R /home/oracle/migration
# mkdir -p /var/TKLC/log/ixp
# chown oracle:oinstall /var/TKLC/log/ixp
```

18. As **oracle** user execute the following commands and scripts to create the Oracle DWS users and schema:

```
# cd /home/oracle/migration/oracle/instance/cmd/
```

a. for **PIC 10.1.5:**

```
# ./createUserTbsp.sh sys/******    (replace ****** by sys password)

# ./installExtDWS.sh ixp/****** sys/******      (replace ****** by ixp and sys user password)
```

b. for PIC 10.2.x onwards:

```
# ./createUserTbsp.sh              (The following steps assume you the user name you created is IXP)

# ./installExtDWS.sh IXP IP_of_DWS_Server IXP
```

19. Extend the tablespaces created in previous steps, per default the choice is to use 90% of the available space, but it can be customize if you wish to save some space to install PIC MGMT application for example. This script will run for multiple hours depending on the server speed so make sure it is executed from a local console access.

    Before extending the data and index tablespaces, the IXP user must be granted DBA privileges. The DBA privileges must be revoked after extension of the tablespaces.

    a. Grant DBA Privileges to IXP database user

Login as sysdba and grant DBA access to IXP database user

```
# sqlplus / as sysdba

>GRANT DBA TO IXP;

> exit
```

    b. Extend the tablespaces

```
# cd /home/oracle/migration/oracle/utils/cmd/

  a. for PIC 10.1.5: # ./CreateDataAndIndexFile.sh -c ixp/****** -p 90 -r

  b. for PIC 10.2.x onwards:    # ./CreateDataAndIndexFile.sh IXP IP_of_DWS_Server IXP -p 90 –r
```

    c. Revoke the DBA privileges from IXP database user

Login as sysdba and revoke DBA access from IXP database user

```
# sqlplus / as sysdba

> REVOKE DBA FROM IXP;

> GRANT UNLIMITED TABLESPACE TO IXP;

> exit
```

20. Once the previous script has finished extending the tablespaces, the server will be ready to receive data from an IXP server. Refer to NSP configuration documentation to create a DatawareHouse pool or add it inside an existing DatawareHouse pool and start writing data into it.

7. PDU STORAGE INSTALLATION ON THIRD PARTY SERVER

Purpose

This chapter explains how to install a PIC Packet Data Unit Storage (PDU) Server on a third party server with Oracle Linux.

This chapter can be applied on a server with Oracle Linux installed using procedure from "Oracle Linux" chapter.

The software versions used for this document are Oracle Linux 7.x (latest update 9) 64bit, Oracle Performance Intelligence Center 10.4.0.

Configure Server for PDU Storage

1. Use a ssh client to access the server via the IP you configured during Oracle Linux installation
2. As **root** user, configure Oracle Linux firewall to accept external connection to Oracle database:

```
# firewall-cmd --permanent --zone=public   --add-service=nfs
# firewall-cmd --permanent --add-port=111/tcp
# firewall-cmd --permanent --add-port=2049/tcp
# firewall-cmd --permanent --add-port=111/udp
# firewall-cmd --permanent --add-port=2049/udp
# firewall-cmd --permanent --add-port=20048/udp
# firewall-cmd --reload
```

3. Create a config user called cfguser to own and share the nfs mounts:

```
# groupadd cfg -g 2000;useradd -d /home/cfguser -g cfg -u 2000 cfguser;passwd cfguser (Enter a password of your choice for cfguser user)
# mkdir -pv /pdu_0
```

4. Create a partition with the RAID 10 logical drive created during Oracle Linux installation and format it, refer System Partitioning Recommendation for the partition recommendation:
    a. As **root** user, use parted to create one partition based on the RAID 10 logical drive built during Oracle Linux installation. The following example is for logical drive is called /dev/sdb

    ```
    # parted /dev/sdb mklabel gpt
    # parted /dev/sdb mkpart primary 0GB 1998GB
    ```

    Once you are done you will have one partition called /dev/sdb1.

    b. Format the partition using mkfs utility:

    ```
    # mkfs.xfs /dev/sdb1
    ```

5. Edit /etc/fstab and add the following line:

```
/dev/sdb1      /pdu_0                  xfs     defaults        0 0
```

6. Mount the partition:

```
# mount /pdu_0
```

7. Change *owner:*

```
chown -R cfguser:cfg /pdu_0
```

8. Edit /etc/exports and add the following line:

```
/pdu_0 ixp????-??(rw,sync)
```

9. Prevent NFSv4 connections:
    a. Edit file /etc/sysconfig/nfs
    b. Change line

```
RPCNFSDARGS=""
```

    to

```
RPCNFSDARGS="--no-nfs-version 4"
```

10. Activate the nfs modifications:

```
# systemctl enable nfs-server
# systemctl restart nfs-server
# exportfs -ra
```

11. Edit /etc/hosts and add the IPs and hostnames of the IXP servers that are going to connect to the PDU server.
12. as **cfguser** create the write.enable file:

```
#date >/pdu_0/write.enable
```

8. MANAGEMENT SERVER (NSP) INSTALLATION ON THIRD-PARTY SERVER

Applies To

Oracle Communications Performance Intelligence Center (PIC) Software - Release 10.4.0 Information in this chapter applies to any platform.

Purpose

This document explains how to install the oracle instance and schema mandatory for to build a Management Server (NSP) 10.4.0 on a third-party server with Oracle Linux.

This chapter is applicable on a server with Oracle Linux 7.x (latest update 9) installed using: "Oracle linux on Third-Party Server Installation Guide for Performance Intelligence Center (PIC) products" and pre-configured with "Oracle 19c ASM and Database on Third-Party Server Installation Guide for Performance Intelligence Center (PIC) Products"

This is a generic installation guide, it can be adapted to match other hardware configurations and/or to new software releases when they will be available.

Scope

The software versions used for this document are Oracle Linux 7.x (latest update 9) 64bit, Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 – (Production Version 19.3.0.0.0) 64bit and Oracle Performance Intelligence Center 10.4.0.

This guide is based on a HP DL380 Gen 9 server configuration. The recommended hardware configuration description can be found in PIC 10.4.0 Hardware Installation Guideline

Prepare for Installation

Note: Use the load lineup from the release notice document for the correct build version

- We recommend to use Edelivery: https://edelivery.oracle.com/ to download Oracle Performance Intelligence Center software as well as Weblogic Server enterprise Edition (FMW, WLS, WeblogicServer 12c) for platform Linux x86-64 V138466-01.zip (containing fmw_12.2.1.4.0_wls.jar) or, for PIC, use the latest patch available on MOS 1989320.2
- We recommend using MOS to download patch 20894426 for Linux x86-64. The zip Archive p20894426_121300_Linux-x86-64.zip contains mod_wl_24.so weblogic plug-in compatible with Apache 2.4.
- We recommend to use MOS KM 1412103.2 to download the latest JDK/JRE 8 update, the zip file downloaded should contain a file called jdk-8uXX-linux-x64.tar.gz (XX will change each time a new version is released, please use the last one available).
- For upgrade, verify size of NSP_LOG tablespace and extended it before importing Oracle backup

Create NSP Database and deploy NSP schema

1. As **root** user Install expect and net snmp packages (make sure you configured the local yum repository and mounted the oracle linux iso as explained in Chapter 4)

```
# mount -o loop /var/ORCL/V*.iso /mnt/repository
# yum install expect net-snmp net-snmp-utils dos2unix
```

2. Update /home/oracle/.bash_profile and add the following lines:

IMPORTANT NOTE: If you have already installed Data WareHouse Server (DWS) application on this server then DO NOT add these lines in /home/oracle/.bash_profile. Just type in the same commands in a shell as oracle user (make sure you do so every time you open a new shell as oracle during this procedure).

```
export ORACLE_SID="NSP"
export ORACLE_INST="NSP"
export ORACLE_UNQNAME="NSP"
```

3. As **oracle** user reload oracle profile:

```
# export ORACLE_SID="NSP"
# export ORACLE_INST="NSP"
# export ORACLE_UNQNAME="NSP"
```

4. Create default directory for NSP database:

```
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/adump
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/pfile
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/cdump
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/bdump
# mkdir -pv $ORACLE_BASE/admin/$ORACLE_SID/udump
# mkdir -pv $ORACLE_BASE/oradata/$ORACLE_SID/flash_recovery_area
# mkdir -pv $ORACLE_BASE/redo/$ORACLE_SID
# mkdir -pv $ORACLE_BASE/oraindex/$ORACLE_SID
# mkdir -pv $ORACLE_BASE/logs
```

5. Create Oracle password file (please customize the password):

```
# orapwd force=y file=$ORACLE_HOME/dbs/orapw$ORACLE_SID password=Tekelec1$
```

6. Copy the initNSP193c.ora to /u01/app/oracle/product/19.3.0/dbhome_1/dbs/:

Edit the init file and customize the "memory_target=" parameter depending on the amount of physical memory available on you server: for example use 16GB on a server containing 32GB of physical RAM, Refer to Oracle Data Administrator Guide for details.

Note : initNSP193c.ora is available here [ initNSP193c.ora]

7. Rename oracle init file:

```
# cp /u01/app/oracle/product/19.3.0/dbhome_1/dbs/initNSP193c.ora /u01/app/oracle/product/19.3.0/dbhome_1/dbs/initNSP.ora
```

8. Connect to sqlplus:

```
# sqlplus / as sysdba
```

9. Startup the database in NOMOUNT:

```
# startup NOMOUNT
```

10.Create Database NSP:

```
CREATE DATABASE NSP
      CONTROLFILE REUSE
      LOGFILE GROUP 1 ('+DATA') SIZE 10G,
            GROUP 2 ('+DATA') SIZE 10G,
            GROUP 3 ('+DATA') SIZE 10G,
            GROUP 4 ('+DATA') SIZE 10G
      DATAFILE '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 8G,
            '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 8G
            EXTENT MANAGEMENT LOCAL
      SYSAUX DATAFILE '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 8G,
            '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 8G
      DEFAULT TEMPORARY TABLESPACE temp
            TEMPFILE '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 2G,
                  '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 2G,
                  '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 2G,
                  '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 2G
                  EXTENT MANAGEMENT LOCAL UNIFORM SIZE 10M
      UNDO TABLESPACE undo
            DATAFILE '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 2G,
                  '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 2G,
                  '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 2G,
                  '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 2G
      CHARACTER SET AL32UTF8
      SET TIME_ZONE = 'America/New_York';
```

11.Create Tablespaces:

```
   CREATE TABLESPACE NSP_conf
   DATAFILE
      '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 2048M,
      '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 2048M
   EXTENT MANAGEMENT LOCAL AUTOALLOCATE
   SEGMENT SPACE MANAGEMENT AUTO;

   CREATE TABLESPACE NSP_log
   DATAFILE
      '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M,
      '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M,
      '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M,
      '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M,
      '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M,
```

```
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M
  EXTENT MANAGEMENT LOCAL AUTOALLOCATE
  SEGMENT SPACE MANAGEMENT AUTO;

  CREATE TABLESPACE NSP_data
  DATAFILE
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M,
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M,
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M,
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 8192M
  EXTENT MANAGEMENT LOCAL AUTOALLOCATE
  SEGMENT SPACE MANAGEMENT AUTO;

  CREATE TABLESPACE NSP_expt
  DATAFILE
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 16384M,
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 16384M,
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 16384M,
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 16384M,
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 16384M,
    '+DATA' SIZE 50M REUSE AUTOEXTEND ON NEXT 50M MAXSIZE 16384M
  EXTENT MANAGEMENT LOCAL AUTOALLOCATE
  SEGMENT SPACE MANAGEMENT AUTO;

  CREATE TABLESPACE NSP_CACHE
  DATAFILE
    '+DATA' SIZE 1024M REUSE AUTOEXTEND ON NEXT 1024M MAXSIZE 20480M,
    '+DATA' SIZE 1024M REUSE AUTOEXTEND ON NEXT 1024M MAXSIZE 20480M,
    '+DATA' SIZE 1024M REUSE AUTOEXTEND ON NEXT 1024M MAXSIZE 20480M,
    '+DATA' SIZE 1024M REUSE AUTOEXTEND ON NEXT 1024M MAXSIZE 20480M,
    '+DATA' SIZE 1024M REUSE AUTOEXTEND ON NEXT 1024M MAXSIZE 20480M
  EXTENT MANAGEMENT LOCAL AUTOALLOCATE
  SEGMENT SPACE MANAGEMENT AUTO;
```

12.Execute sql scripts:

```
@$ORACLE_HOME/rdbms/admin/catalog.sql
@$ORACLE_HOME/rdbms/admin/catblock.sql
@$ORACLE_HOME/rdbms/admin/catproc.sql
@$ORACLE_HOME/rdbms/admin/dbmspool.sql
exit
```

13. Set the ‘system’ user password.

```
# sqlplus / as sysdba
alter user system identified by system_user_password;          <<replace system_user_password with password>>
exit
```

Exit sqlplus and log as system user:

```
# sqlplus system/******          (replace ****** by system user password)
```

```
@$ORACLE_HOME/sqlplus/admin/pupbld.sql
exit
```

14. Log back as sysdba and create NSP users:

```
# sqlplus / as sysdba

      CREATE USER NSP
      IDENTIFIED BY NSP          <<IF THIS IS AN UPGRADE MAKE SURE YOU ARE USING THE PASSWORD
STORED IN THE WALLET FOR NSP USER>>
      DEFAULT TABLESPACE NSP_conf
      TEMPORARY TABLESPACE temp;

GRANT CONNECT TO NSP;
GRANT RESOURCE TO NSP;
GRANT DBA TO NSP;
GRANT SELECT ON DBA_FREE_SPACE TO NSP;
GRANT SELECT ON DBA_DATA_FILES TO NSP;
GRANT UNLIMITED TABLESPACE TO NSP;
CREATE OR REPLACE DIRECTORY DBG_DIR AS '/var/log/nsp';
GRANT READ,WRITE ON DIRECTORY DBG_DIR TO PUBLIC;
GRANT READ,WRITE ON DIRECTORY DBG_DIR TO NSP;
CREATE OR REPLACE    DIRECTORY BACKUP_DIR AS    '/opt/backup/backup';
GRANT READ,WRITE ON DIRECTORY BACKUP_DIR TO PUBLIC;
GRANT READ,WRITE ON DIRECTORY BACKUP_DIR TO NSP;
ALTER USER NSP DEFAULT ROLE ALL;
ALTER PROFILE DEFAULT LIMIT PASSWORD_LIFE_TIME UNLIMITED;
ALTER SYSTEM SET SEC_CASE_SENSITIVE_LOGON=TRUE;

CREATE USER NSP_LOG
    IDENTIFIED BY NSP_LOG
    DEFAULT TABLESPACE NSP_conf
    TEMPORARY TABLESPACE temp;
GRANT CREATE SESSION TO NSP_LOG;
exit
```

15. Copy the CreateAndAttachUserProfile.sh, CreateAndAttachUserProfile.sql, CreatePasswordVerificationFunction.sql to /u01/app/oracle/product/19.3.0/dbhome_1/dbs/:

```
cd /u01/app/oracle/product/19.3.0/dbhome_1/dbs/
chmod 777 CreateAndAttachUserProfile.sh
chown oracle:oinstall CreateAndAttachUserProfile.sh
chown oracle:oinstall CreateAndAttachUserProfile.sql
chown oracle:oinstall CreatePasswordVerificationFunction.sql

(As an oracle user)
./CreateAndAttachUserProfile.sh NSP/<PASSWORD>@NSP NSP NSP
```

16. Wait 2 minutes and verify that listener is seeing NSP and ASM instances:

```
# lsnrctl status
```

Expected output:

```
Service "+ASM" has 1 instance(s).
  Instance "+ASM", status READY, has 1 handler(s) for this service...
Service "NSP" has 1 instance(s).
  Instance "NSP", status READY, has 1 handler(s) for this service...
The command completed successfully
```

16. Create spfile:

```
# sqlplus / as sysdba

shutdown immediate

create spfile from pfile;
startup mount
alter database open;
alter system register;
shutdown immediate
exit
```

17.Register Oracle Database with has:

```
# srvctl add database -d $ORACLE_SID -o $ORACLE_HOME -n $ORACLE_SID -a "DATA"
```

18.Start Oracle database with has:

```
# srvctl start database -d $ORACLE_SID -o OPEN
```

19.Provide privileges to NSP user :

```
# sqlplus / as sysdba

ALTER SYSTEM SET SEC_CASE_SENSITIVE_LOGON = TRUE SCOPE = SPFILE;
ALTER SYSTEM SET GLOBAL_NAMES = FALSE SCOPE = SPFILE;
ALTER SYSTEM SET REMOTE_LOGIN_PASSWORDFILE = 'EXCLUSIVE' SCOPE = SPFILE;
ALTER SYSTEM SET SQL92_SECURITY = FALSE SCOPE = SPFILE;

GRANT SELECT ON DBA_FREE_SPACE TO NSP;
GRANT SELECT ON DBA_DATA_FILES TO NSP;
GRANT SELECT ON DBA_SEGMENTS TO NSP;
GRANT CONNECT TO NSP;
GRANT CREATE TABLE TO NSP;
GRANT CREATE ROLE TO NSP;
GRANT CREATE SEQUENCE TO NSP;
GRANT CREATE PROCEDURE TO NSP;
GRANT CREATE TRIGGER TO NSP;
GRANT CREATE PUBLIC SYNONYM TO NSP;
GRANT GRANT ANY ROLE TO NSP;
GRANT GRANT ANY PRIVILEGE TO NSP;
```

```
GRANT DROP ANY TRIGGER TO NSP;
GRANT DROP ANY ROLE TO NSP;
GRANT DROP PUBLIC SYNONYM TO NSP;
GRANT ADMINISTER DATABASE TRIGGER TO NSP;
GRANT UNLIMITED TABLESPACE TO NSP;
GRANT ANALYZE ANY TO NSP;
GRANT EXECUTE ON DBMS_LOCK TO NSP;
GRANT EXECUTE ON SYS.DBMS_SHARED_POOL TO NSP;
GRANT SELECT ON DBA_JOBS TO NSP;
GRANT SELECT ON DBA_JOBS_RUNNING TO NSP;
GRANT EXECUTE ON DBMS_JOB TO NSP;
GRANT CREATE ANY DIRECTORY TO NSP;

REVOKE EXECUTE ON DBMS_ADVISOR FROM PUBLIC;
REVOKE EXECUTE ON DBMS_JOB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LDAP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHEDULER FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLGEN FROM PUBLIC;
REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;
REVOKE EXECUTE ON UTL_INADDR FROM PUBLIC;
REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;
REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;
REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;

GRANT EXECUTE ON DBMS_JOB TO NSP,NSP_LOG,DBSNMP,SYSTEM;
GRANT EXECUTE ON DBMS_LOB TO NSP,NSP_LOG;
GRANT EXECUTE ON DBMS_OBFUSCATION_TOOLKIT TO NSP,NSP_LOG,DBSNMP,SYSTEM;
GRANT EXECUTE ON DBMS_SCHEDULER TO NSP,NSP_LOG,DBSNMP,SYSTEM;
GRANT EXECUTE ON DBMS_SQL TO NSP,NSP_LOG,DBSNMP,SYSTEM;
GRANT EXECUTE ON UTL_FILE TO NSP,NSP_LOG,DBSNMP,SYSTEM;
GRANT EXECUTE ON UTL_TCP TO DBSNMP,SYSTEM;
GRANT EXECUTE ON UTL_SMTP TO DBSNMP,SYSTEM;
GRANT EXECUTE ON DBMS_LOB TO XDB;
GRANT EXECUTE ON UTL_FILE TO XDB;
GRANT EXECUTE ON DBMS_SQL TO XDB;
GRANT EXECUTE ON DBMS_JOB TO XDB;
GRANT EXECUTE ON DBMS_STATS TO XDB;
GRANT EXECUTE ON UTL_RAW    TO XDB;
GRANT CREATE JOB TO NSP;

exit
```

20.Reset oracle sys password for installation :

```
# sqlplus / as sysdba

alter user sys identified by oracle;
```

21. Oracle NSP database is now ready.

Install Java JDK,weblogic and NSP applications

1. As **root** create Tekelec user and default folders:

```
# groupadd tekelec;useradd -m -u 5020 -d /opt/nsp -g tekelec tekelec;passwd tekelec
(Enter a password of your choice for tekelec user)

# usermod -a -G oinstall tekelec
# chmod 755 /opt/nsp/
# chown -R tekelec:tekelec /opt/nsp
# mkdir -p /opt/oracle/bea
# mkdir -p /opt/nsp/wl_tmp
# mkdir -p /opt/nsp/temp
# mkdir -p /mnt/upgrade
# chown -R tekelec:tekelec /opt/oracle/
# chown -R tekelec:tekelec /opt/nsp/temp
# chown -R tekelec:tekelec /opt/nsp/wl_tmp
# mkdir -p /opt/backup/backup
# chown -R tekelec:tekelec /opt/backup/backup
```

2.Copy jdk-8uXX-linux-x64.tar.gz, fmw_12.2.1.4.0_wls.jar and PIC-MGMT-10.4.0.c.d_x.y.z-x86_64.iso to /var/ORCL and mount PIC-MGMT iso to /mnt/upgrade:

```
# mount -o loop /var/ORCL/PIC-MGMT-10.*-x86_64.iso /mnt/upgrade
```

3.Unzip nsp-package :

```
# unzip -q -o -d /opt/nsp/nsp-package   /mnt/upgrade/nsp/nsp-package.zip
```

4.Unzip jdk to /opt/nsp :

```
# tar zxvf /var/ORCL/jdk-8u*-linux-x64.tar.gz -C /opt/oracle/
```

5. Copy wl_silent.txt to /tmp:

```
cp /mnt/upgrade/scripts/wl_silent.txt /tmp
```

If you like to install weblogic software in a specific directory other than /opt/oracle/bea you need to edit /tmp/wl_silent.txt and update ORACLE_HOME variable, that specific directory must be owned by tekelec user.

6.Install Weblogic software :

```
# su - tekelec -c "/opt/oracle/jdk1.8*/bin/java -Djava.io.tmpdir=/opt/nsp/wl_tmp -d64 -jar /var/ORCL/fmw_12.2*_wls.jar -silent -responseFile /tmp/wl_silent.txt -invPtrLoc /u01/app/oraInventory/oraInst.loc"
```

7.Create symbolic links to BEA_HOME:

```
# export BEA_HOME=/opt/oracle/bea
# ln -s /opt/oracle/jdk1.8.* $BEA_HOME/jdk
# ln -s $BEA_HOME/wlserver/ $BEA_HOME/wlhome
# mkdir -p $BEA_HOME/wlhome/common/nodemanager
```

```
# ln -s $BEA_HOME/oracle_common/common/bin/commEnv.sh $BEA_HOME/wlhome/common/bin/commEnv.sh
# ln -s $BEA_HOME/wlhome/common/nodemanager $BEA_HOME/oracle_common/common/nodemanager
# chown tekelec:tekelec $BEA_HOME/jdk $BEA_HOME/wlhome/common/nodemanager
```

8. Create a partition on logical drive created to store the NSP daily backup

Replace /dev/sdX with the correct logical drive created during Chapter 4 and adjust partition size to match the logical drive size. If you are performing an upgrade skip these steps and go to step 10

```
# parted /dev/sdX mklabel gpt
# parted /dev/sdX mkpart primary 0GB 900GB
```

9.Format the newly created partition:

```
# mkfs.xfs /dev/sdX1
```

10.Edit /etc/fstab and add the backup mount point

```
/dev/sdX1 /opt/oracle/backup        xfs   defaults        1 2
```

11.Create backup directory to store NSP daily backup and mount it

```
# mkdir -pv /opt/oracle/backup;mount /opt/oracle/backup
```

12.Install NSP software (installation will take some time, we recommend running it from ILO,you can monitor its progress in /var/log/nsp/install/nsp_install.log)

```
# export BEA_HOME=/opt/oracle/bea
```

In case of fresh install, perform the following command:

Note: Follow the Oracle Secure password guidelines for setting up the database password. The password may only contain special characters from # ! % ^ & * ( ) _ + - { } [ ] ; : . , < > ? ~

```
# sh /mnt/upgrade/install_nsp.sh
```

In case of upgrade, make sure the NSP backup NSP_BACKUP_XX_XX_XX_XX_XX_XX is present in /opt/oracle/backup and perform the following command:

Note: The last NSP backup directory going to be use for db import and realm import, make sure the correct backup directory in place.

```
# ls -dtr /opt/oracle/backup/NSP* | tail -1
# chown oracle:oinstall /opt/oracle/backup/NSP_BACKUP_XX_XX_XX_XX_XX_XX/ExpNSP.dmp.gz
# sh /mnt/upgrade/upgrade_nsp.sh
```

Verify the upgrade is fine using the **Step 3** of the procedure "**Management Server Pre-Upgrade Healthcheck and Settings**" in 10.4 Upgrade Guide

13. When prompted provide the following answers:

In case of install/upgrade the script will ask for oracle NSP user password and ask you to confirm.

Note: Follow the Oracle Secure password guidelines for setting up the database password. The password may only contain special characters from # ! % ^ & * ( ) _ + - { } [ ] ; : . , < > ? ~

```
Enter server name for Admin server :nspadmin
Enter server name for managed server 1 :nsp1a
Enter server name for managed server 2 :nsp1b
Enter password for wallet : Tekelec1$ (any value can be used but keep it safe as you will need it later)
05-Apr-2017 05:05 ---INFO : Wallet created successfully
Enter the database user name :NSP
Enter the database service name :NSP
Enter the IP of database server (default: localhost) :10.20.30.40 (specify the backend IP of the server you are installing)
Enter old password : (the old password is NSP)
Enter new password : (any value can be used but keep it safe as you will need it later)
Confirm new password : (any value can be used but keep it safe as you will need it later)
Enter password for wallet : (enter the value that you set on the first request for wallet password)
05-Apr-2017 05:07 ---BEGIN: modifyPassword.sh for 10.20.30.40 with user nsp.
05-Apr-2017 05:07 ---WARN : Old and new passwords are same.
05-Apr-2017 05:07 ---INFO : Proceeding with database credential check.
05-Apr-2017 05:07 ---INFO : Old password is verified successfully. Going to change password.
Enter password for sys : oracle (default is oracle as set in step 21 of previous chapter)
```

14. As **root** user, once the installation is completed, disable dbora service:

```
# chkconfig --level 345 dbora off
```

15**. Fix th**e permission on weblogic instance logs :# chmod 755 /opt/oracle/bea/user_projects/domains/tekelec/servers/nsp1a/logs/
chmod 755 /opt/oracle/bea/user_projects/domains/tekelec/servers/nsp1b/logs/

Install Apache(httpd) as NSP front end

1.As root user install httpd and mod_ssl: (make sure you configured the local yum repository and mounted the oracle linux iso as explained in Chapter 4)

```
# mount -o loop /var/ORCL/V*.iso /mnt/repository
# yum install httpd
# yum install mod_ssl.x86_64
```

2. Extract mod_wl_24.so from p20894426_121300_Linux-x86-64.zip and copy it to /var/ORCL.

3. Copy mod_wl_24.so to /etc/httpd/modules:

```
# cp /var/ORCL/mod_wl_24.so /etc/httpd/modules/
```

4. Configure weblogic plugin for apache:

```
Copy the attached wl_24.conf to /etc/httpd/conf.d
```

Note: wl_24.conf is available here [ wl_24.conf].

Edit /etc/httpd/conf.d/wl_24.conf and replace "BACKEND_of_MGMT" by the backend IP address of the MGMT server.

5. Add ***HTTP security headers***

```
# Edit /etc/httpd/conf/httpd.conf, using any editor e.g. vi
# Add/update the following content in the httpd.conf file

<IfModule mod_headers.c>
<Directory />
Header always set X-XSS-Protection "1; mode=block"
Header always set x-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
Header always set Strict-Transport-Security "max-age=16070400; includeSubDomains"
</Directory>
</IfModule>

<If "%{HTTPS} == 'on'">
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure;
</If>

# Save the httpd.conf file.
```

6.Enable and start httpd service

```
# systemctl enable httpd;systemctl start httpd
```

7. Create symbolic link for online documentation

```
# mv /var/www/html /var/www/html.old
# ln -s /opt/www /var/www/html
```

8. The Apache Server is now up and running and the NSP GUI can be reached from the front end IP address.

9. Reboot the server.

Management Server Post Installation Configuration

1. Refer to PIC Installation guide to perform Post Installation customization:
    a. Change Customer Icon (Optional)
    b. Install Optional Applications
    c. Configure Purchased Tokens
2. Refer to PIC Maintenance Guide to perform Post Installation configuration:
    a. Configure Mail Server (Optional)
    b. Configure Authenticated Mail Server (Optional)

c. Configure SNMP Management Server (Optional) snmpd service needs to be enabled as **root** user:

```
#systemctl enable snmpd;service jmxd restart
```

3. Refer to PIC Upgrade Guide to perform Post Installation configuration:
    a. Post-Upgrade Settings
    b. Management Server Backup
    c. Unset Configuration on Management Server
    d. Upload xDR Builder ISO to Management Server (**if some errors are generated execute "chmod -R 755 /opt/nsp/builder/" as root and try again**)

Secure the operating system, referring to Oracle Linux 7 Security Guide , and especially Restricting Access to SSH Connections

Management Server Post Install Health Check

1. Open a terminal window and log in as root on the Management Server.
2. Review the Management Server installation logs (/var/log/nsp/install/nsp_install.log).
3. Log on to weblogic console and Verify the following:
    - All servers are in running and in OK state
    - Application deployments are in Active and OK state.

Revoke DBA role from NSP user

1. Login to NSP machine and change user to oracle by command:

```
# su - oracle
```

2. Login to sqlplus console using command:

```
# export ORACLE_SID=NSP
# ORAENV_ASK=NO source oraenv
# sqlplus / as sysdba
```

3. Execute command to revoke DBA and grant necessary privilege from NSP user

```
> REVOKE DBA FROM NSP;
> GRANT CREATE ANY DIRECTORY TO NSP;
> GRANT UNLIMITED TABLESPACE TO NSP;
> GRANT CREATE DATABASE LINK TO NSP;
> GRANT CREATE ANY VIEW TO NSP;
```

Note: Ignore errors if any.

Execute below command to confirm that DBA role has been revoked from NSP user or not

```
> SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'NSP';
GRANTED_ROLE
------------
RESOURCE
CONNECT
```

If the result of above command still contains DBA role in result set then refer to Appendix E: My Oracle Support

9. MANAGEMENT SERVER (NSP) INSTALLATION ON TPD SYSTEM

Note: This chapter is now Obsolete and should not be used for any TPD based installation. PIC 10.4 does not support TPD based installation.

Applies To

Oracle Communications Performance Intelligence Center (PIC) Software - Release 10.4.0. Information in this chapter applies to any platform.

Purpose

This document explains how to install a Management Server (NSP) 10.4.0 on a TPD operating system server.

This type of configuration allows customer to keep a complete TPD based PIC system in order to gather hardware and system alarms via the MGMT/NSP alarming system.

Scope

The software versions used for this document are TPD 7.6, Oracle Database 11g Enterprise Edition, Weblogic 12.2c and Oracle Performance Intelligence Center 10.4.0.

This guide is based on a HP DL380 Gen 9 server configuration. The recommended hardware configuration description can be found in PIC 10.4.0 Hardware Installation Guideline.

Details

Prepare for Installation

- We recommend to use edelivery: https://edelivery.oracle.com/ to download Oracle Performance Intelligence Center software as well as Weblogic Server enterprise Edition (FMW, WLS, Weblogic Server 12c) for platform Linux x86-64 V138466-01.zip (containing fmw_12.2.1.4.0_wls.jar) or, for PIC, use the latest patch available on MOS 1989320.2
- We recommend downloading Oracle Database software from MOS to get the latest patch set. This guide is based on Linux x86_64 Patch 13390677: 11.2.0.4.0 PATCH SET FOR ORACLE DATABASE SERVER(p13390677_112040_Linux-x86-64_1of7.zip, p13390677_112040_Linux-x86-64_2of7.zip, p13390677_112040_Linux-x86-64_3of7.zip)

Install TPD server, WebLogic, oracle and NSP/MGMT application

1. Install the TPD operating system following the procedure specific to your hardware type: Refer Chapter 3 System Configuration on TPD for IPM instructions.

If you are using a serial connection to the server you can use **"TPDnoraid console=ttyS0"** and follow the installation from the serial console

2. Wait until the TPD installation finishes and hit the "reboot" button

Execute the next steps from a Non-disconnect able terminal (either KVM, serial or ILO console)

3. As **root** user extend the /var/TKLC partition using the following commands:

```
# init 2
# umount /dev/mapper/vgroot-plat_var_tklc
# lvextend -L +4G /dev/mapper/vgroot-plat_var_tklc
# e2fsck -f /dev/mapper/vgroot-plat_var_tklc
# resize2fs -p /dev/mapper/vgroot-plat_var_tklc
# reboot
```

4. Once the server has rebooted, log back as root user and execute the following command:

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit
```

5. Transfer the installation files to the server in /var/TKLC/upgrade folder, this includes the PIC MGMT 10.4.0 iso, the weblogic "fmw_12.2*_wls.jar", the java jdk "jdk-8u*.tar.gz" and the 3 oracle zip installation files "p13390677_112040_Linux-x86-64*zip"

6. Create NSP bulkconfig following the recommendation in the "PIC MGMT Server bulkconfig file description"

7. Mount the PIC MGMT iso in /mnt/upgrade:

```
# mount -o loop /var/TKLC/upgrade/PIC-MGMT-10.4.0*.iso /mnt/upgrade
```

8. Installed rpm package:

```
# rpm -ivh /mnt/upgrade/Packages/ed*.rpm
```

9. Install oracle binary:

```
# /mnt/upgrade/install_oracle.sh
```

10. Once the server has rebooted, verify the content of /etc/hosts an make sure there is **one** line containing the IP and hostname of the server. If not please add a line containing only the IP address and the hostname
11. Mount the PIC MGMT iso in /mnt/upgrade:

```
# mount -o loop /var/TKLC/upgrade/PIC-MGMT-10.4.0*.iso /mnt/upgrade
```

12. Install Oracle Database (this will take a long time, you can monitor the progress in /var/log/nsp/install/nsp_install.log):

```
# rpm -ivh –nodeps /mnt/upgrade/Packages/oracle-11.2.0.4-1.0.0.x86_64.rpm
```

13. As **oracle** user change the sys user password (**mandatory**):

```
# sqlplus / as sysdba
SQL> alter user sys identified by oracle;
SQL> exit
```

14. As **root** user, execute the following commands to install weblogic:

```
# usermod -a -G oinstall tekelec
# mkdir -p /opt/nsp/wl_tmp;mkdir -p /opt/nsp/bea;mkdir -p /opt/nsp/ant
# chmod 755 /opt/nsp/
# chown tekelec:tekelec /opt/nsp/wl_tmp;chown tekelec:tekelec /opt/nsp/bea;chown tekelec:tekelec /opt/nsp/ant
# tar zxvf /var/TKLC/upgrade/jdk-8u*-linux-x64.tar.gz -C /opt/nsp
# cp /mnt/upgrade/scripts/wl_silent.txt /tmp
# chmod 777 /tmp/wl_silent.txt
# sed -i "s:/opt/oracle/bea:/opt/nsp/bea:g" /tmp/wl_silent.txt
# su - tekelec -c "/opt/nsp/jdk1.8*/bin/java -Djava.io.tmpdir=/opt/nsp/wl_tmp -d64 -jar /var/TKLC/upgrade/fmw_12.2*_wls.jar -silent -responseFile /tmp/wl_silent.txt -invPtrLoc /usr/TKLC/oracle11/oraInventory/oraInst.loc"
```

15. Copy the attached startNSP.sh in /tmp folder and change the permissions. Note : startNSP.sh is available here [].


```
# chmod 777 /tmp/startNSP.sh
```

16. Copy the attached install_nsp_TPD74.sh to /tmp and change the permissions. Note : install_nsp_TPD74.sh is available here [].


```
# dos2unix /tmp/install_nsp_TPD74.sh;chmod +x /tmp/install_nsp_TPD74.sh
```

17. Execute install_nsp_TPD74.sh and provide answers to the script request (script execution is very long, it can take more than 2 hours)

```
# /tmp/install_nsp_TPD74.sh
```

Executed output:

```
Enter server name for Admin server :nspadmin
Enter server name for managed server 1 :nsp1a
Enter server name for managed server 2 :nsp1b
Enter password for wallet : Tekelec1$       (any value can be used but keep it safe as you will need it later)
05-Apr-2017 05:05 ---INFO : Wallet created successfully
Enter the database user name :nsp
Enter the database service name :nsp
Enter the IP of database server (default: localhost) :10.20.30.40     (specify the backend IP of the server you are installing)
Enter old password :                          (the old password is nsp)
Enter new password :                          (any value can be used but keep it safe as you will need it later)
Confirm new password :                        (any value can be used but keep it safe as you will need it later)
Enter password for wallet :                   (enter the value that you set on the first request for wallet password)
05-Apr-2017 05:07 ---BEGIN: modifyPassword.sh for 10.20.30.40 with user nsp.
05-Apr-2017 05:07 ---WARN : Old and new passwords are same.
05-Apr-2017 05:07 ---INFO : Proceeding with database credential check.
05-Apr-2017 05:07 ---INFO : Old password is verified successfully. Going to change password.
Enter password for sys : oracle              (default is oracle as set in step 13)
```

18.Monitor installation progress by tailing nsp_install.log:

```
# tail -f /var/log/nsp/install/nsp_install.log
```

19. Reboot the server:

```
# reboot
```

20. Log a **root** user and restrict ssh root access:

```
# /usr/TKLC/plat/sbin/rootSshLogin –revoke
```

Management Server Post Installation Configuration

1. Refer to PIC Installation guide to perform Post Installation customization:
    a. Change Customer Icon (Optional)
    b. Install Optional Applications
    c. Configure Purchased Tokens
2. Refer to PIC Maintenance Guide to perform Post Installation configuration:
    a. Configure Mail Server (Optional)
    b. Configure Authenticated Mail Server (Optional)
    c. Configure SNMP Management Server (Optional)
3. Refer to PIC Upgrade Guide to perform Post Installation configuration:
    a. Post-Upgrade Settings
    b. Management Server Backup
    c. Unset Configuration on Management Server"
    d. Upload xDR Builder ISO to Management Server (if some errors are generated execute "chmod -R 755 /opt/nsp/builder/" as root and try again)

Management Server Post Install Health Check

1. Open a terminal window and log in as root on the Management Server.
2. Review the Management Server installation logs (/var/log/nsp/install/nsp_install.log).
3. Log on to weblogic console and Verify the following:
    - All servers are in running and in OK state
    - Application deployments are in Active and OK state.

Revoke DBA role from NSP user

1. Login to NSP machine and change user to oracle by command:

    ```
    # su - oracle
    ```

2. Login to sqlplus console using command:

    ```
    # export ORACLE_SID=NSP
    # ORAENV_ASK=NO source oraenv
    # sqlplus / as sysdba
    ```

3. Execute command to revoke DBA and grant necessary privilege from NSP user

```
> REVOKE DBA FROM NSP;
> GRANT CREATE ANY DIRECTORY TO NSP;
> GRANT UNLIMITED TABLESPACE TO NSP;
> GRANT CREATE DATABASE LINK TO NSP;
> GRANT CREATE ANY VIEW TO NSP;
```

Note: Ignore errors if any.

Execute below command to confirm that DBA role has been revoked from NSP user or not

```
> SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'NSP';
GRANTED_ROLE
------------
RESOURCE
CONNECT
```

If the result of above command still contains DBA role in result set then refer to Appendix E: My Oracle Support

10. ACQUISITION APPLICATION INSTALLATION

This section provides the procedures for installing the acquisition server application.

For a probed acquisition, make sure that the appropriate cards for the traffic capture are physically installed in the server inside standard PCI slots and not on reserved Flex Lom slot. In such way, the two cards are seen inside slot 1 and 2, this result the Ethernet ports seen are eth11-14 and eth21-24 (and not has eth0X when insert in Flex Lom slots).

Note: This step should be executed for all the servers in sub-system.

Pre-Install Configuration

This section provides procedures to configure the acquisition servers that must be performed before installing the acquisition server application.

Temporary customer IP assignment

This procedure provides instructions to temporary customer IP assignment to transfer the Application

ISO on server during installation.

Note: This procedure is only to be used to transfer the Application ISO during installation.

Configure Vlan tagging and assign ip address in case of Integrated Acquisition Server

1. Login via ILO, iLOM, to server as root
2. Execute following commands (1st line for E5-APP-B only):

```
# ifconfig eth01 up
# modprobe 8021q
# vconfig add eth01 200
# ifconfig eth01.200 <cust_IP_address> netmask <mask>
# route add default gw <default_route_IP_address>
```

Assign ip address in case of Probed Acquisition Server: see Appendix A: Manual configuration of ethernet interfaces

Copy ISO

1. Transfer acquisition server ISO on the server to /var/TKLC/upgrade directory
2. Verify that ISO file is transferred completely on the server.

Configure server

This procedure describes how to configure the acquisition servers prior to installing the application.

Note: This procedure must be executed on all of the Integrated and Probed acquisition servers.

Change the current hostname, designation and function

Note: The designation and function are case sensitive and must be capitalized; otherwise, the software functionality will not work properly and will result in the need to reinstall the application.

1. Enter the platcfg menu, as root run:

```
# su - platcfg
```

2. Select Server Configuration->Hostname
3. Select Edit
4. Set the hostname
5. Select Server Configuration -> Designation/Function.
6. Select Edit.
7. Change the designation and function.
   - For a Integrated Acquisition subsystem:

     In the Designation field, enter the designation in the following format: 1A for the first server, 1B for the second, and so on. In the Function field, enter IMF.
   - For a standalone Probed Acquisition:

     In the Designation field, enter the 0A for the server. In the Function field, enter PMF.
8. Select Exit.

Install the bulkconfig file

1. Login as root user.
2. For creation of /root/bulkconfig file refer section Acquisition Server Bulkconfig File Description.

Acquisition Server Pre-Install Healthcheck

This procedure describes how to run the syscheck and analyze the output to determine the state of the server before installing the acquisition server application.

Log in as root on the server that you want to install the acquisition server application.

Run:

```
# syscheck
```

Review the fail_log file (/var/TKLC/log/syscheck/fail_log) for any errors.

```
Example ouput for a healthy system:
Running modules in class disk...
                                        OK
Running modules in class hardware...
                                        OK
Running modules in class net...
                                        OK
Running modules in class proc...
                                        OK
Running modules in class system...
                                        OK
Running modules in class upgrade...
                                        OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

Install Acquisition Server Application

This procedure describes how to install the acquisition server application on a server that has the operating system installed.

Note: Run this procedure from iLO console

1. Log in as root user
2. Enter the platcfg menu, as root run:

```
# su - platcfg
```

3. Select Maintenance ➤ Upgrade ➤ Initiate Upgrade.
4. Select the acquisition server application media and press Enter.

Informational messages appear on the terminal screen as the upgrade proceeds. When installation is complete, the server reboots and displays the login prompt.

You can check the TPD upgrade log file (/var/TKLC/log/upgrade/upgrade.log) for any error; but the status of the server will be checked when you run the healthcheck script after you configure the switches.

Install JRE

Execute Install JRE 1.8

Configure Site and Subsystem for Acquisition Server

This procedure describes how to create a site on Management Server and set a subsystem in this new site.

The subsystem is treated as a cluster, accessible by Management Server through this IP address.

A dedicated IP address, called Virtual IP (VIP), is needed for the subsystem. This address must be a real address in the subsystem subnet that is not physically used by any other server or equipment. The current Active Master server in the subsystem is the server representing the VIP.

For a standalone Probed Acquisition Server, the VIP is the IP address of the server. For a single-server Integrated Acquisition Server, it is possible to assign the server IP address as VIP; however, when additional servers are added, the VIP address must be changed to a dedicated IP address to work properly. It is recommended that a dedicated IP address be used from the beginning, to avoid changing the VIP when more servers are added.

In this release due to various security enhancements, the generation of oracle wallet and its sync to each of the server in the sub-system is mandatory. The wallet generation and syncing shall be required on every new site/sub-system creation. Refer to Appendix Modify Wallet Password .

Note: There is only one Acquisition subsystem supported per site. If a standalone Probed Acquisition is in a site/subsystem, no other Acquisition subsystem or standalone Probed Acquisition can be added. They need to be added to different logical site in **Centralized Configuration.** All of the configuration is performed through the Management server application interface.

1. Sync Database Credentials

   Execute procedure in Appendix: Sync Database Credentials

   Note: The sync of credentials must be done for all the servers in the acquisition sub-system.

2. Log in to the Management server application

   a. Log in as tekelec to the Management server application interface using the management server IP address.

b. Click **Centralized configuration.**

3. Create a site on CCM

   a. Select **Equipment Registry ► Sites ► Add.**

   b. Type the desired site name and click **Add.**

   Note: Refer to Chapter 5 section Site Creation and Discovery Process of Centralized Configuration Manager Administrator Guide of Performance Intelligence Center for configuring Production and Management Network.

4. Create Acquisition sub-system and Add the server(s) on Management Server

   Note: Skip this step if the Site already exists.

   a. Select **Equipment Registry ► Sites ► *New site name created* ► XMF ► Add** or select ***Equipment Registry ► Sites ► New site name created ► OCDSR ► Add*** for OCDSR

   b. Type the server IP address(es) for the xMF subsystem and click **Add** or for OCDSR type the server IP and the DSR SOAM VIP.

   c. Click **Create.**

   Note: Refer to Chapter 5 section Site Creation and Discovery Process of Centralized Configuration Manager Administrator Guide of Performance Intelligence Center for configuring Production and Management Network.. For adding OCDSR site refer section “Adding An Integrated ODCDSR”.

Acquisition Server Healthcheck post customer integration

This procedure describes how to run the healthcheck script on acquisition servers.

The script gathers the healthcheck information on each server in the acquisition subsystem or from standalone server. The script should be run from each of the server of the acquisition subsystem or on stand-alone. The output consists of a list of checks and results, and, if applicable, suggested solutions.

1. Open a terminal window and log in as cfguser on each server in the acquisition subsystem or standalone server.
2. Run the automatic healthcheck script.

```
$ analyze_server.sh -i
```

3. Analyze the output of the script for errors. Issues reported by this script must be resolved before any further usage of this server. Verify no errors are present.

   If the error occurs, refer to Appendix E: My Oracle Support

   Example output for a healthy server in a subsystem:

```
04:57:30: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
04:57:31: date: 02-26-16, hostname: imf9040-1a
04:57:31: TPD VERSION: 7.6.2.0.0-88.58.0
04:57:31: XMF VERSION: [ 10.4.0.0.0-1.7.0 ]
04:57:32: ------------------------------------------------
04:57:32: Checking disk free space
04:57:32:          No disk space issues found
04:57:32: Checking syscheck - this can take a while
04:57:43:          No errors in syscheck modules
04:57:44: Checking statefiles
```

```
04:57:44:       Statefiles do not exist
04:57:44: Checking runlevel
04:57:45:       Runlevel is OK (4)
04:57:45: Checking upgrade log
04:57:45:       Install logs are free of errors
04:57:45: Analyzing date
04:57:46:       NTP deamon is running
04:57:46:       IP of NTP server is set
04:57:46:       Server is synchronized with ntp server
04:57:47: Analyzing IDB state
04:57:47:       IDB in START state
04:57:47: Checking IDB database
04:57:48:       iaudit has not found any errors
04:57:48: Analyzing processes
04:57:49:       Processes analysis done
04:57:49: Analysing database synchronization
04:57:50:       Either Database synchronization in healthy state or errors found are non-blocking
04:57:50: Checking weblogic server entry
04:57:50:       Appserver is present
04:57:50: All tests passed. Good job!
04:57:51: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
```

Disable eth04 interface on E5-APP-B (Optional)

Execute the procedure Disable interface eth04 on E-5APP-B

Configure Production Network (Optional)

Execute the procedures define in Configure Production Interface

11. MEDIATION APPLICATION INSTALLATION

Mediation Server Pre-Install Configuration

This procedure describes how to configure mediation server prior to installing the application.

Before you perform this procedure, make sure you have read and are familiar with the Mediaion Server Bulkconfig File Description, see Mediation Server Bulkconfig File Description.

Note: When creating a bulkconfig file on a server in the Mediation subsystem, if such a file has already been created on a different server, then reuse that bulkconfig file. The content of the bulkconfig file is the same for all servers in the Mediation subsystem.

Verify each server healthcheck.

1. Run syscheck. Log in as root on the server that you want to install the application. As root run:

```
# syscheck
```

2. Review the /var/TKLC/log/syscheck/fail_log file for any errors.

   Example output of healthy server:

```
Example ouput for a healthy system:
Running modules in class disk...
                                        OK
Running modules in class hardware...
                                        OK
Running modules in class net...
                                        OK
Running modules in class proc...
                                        OK
Running modules in class system...
                                        OK
Running modules in class upgrade...
                                        OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

   Resolve each error before you continue with the procedure.

   Note: Errors of NTP in syscheck can be ignored at this time, as NTP server is not configured

Configure Bonding Interface (Optional)

Note: In case of bonding, if any of the interface is down e.g. eth01 or eth02, then no alarm will be raised by the platform or the application.

1. Login into the mediation server's console
2. To create the bonding interface, as root, run:

```
# netAdm add --device=bond0 --bootproto=none --type=Bonding --addr=<ip-address> --netmask=<network-mask> --
onboot=yes --mode=active-backup --miimon=100 --bondInterfaces=eth01,eth02
```

3. To create the default route, as root, run:

```
# netAdm add --route=default --device=bond0 --gateway=<gateway-ip>
```

Create the bulkconfig file

1. As a root user.
2. Create the /root/bulkconfig file as explained in Appendix Mediation Server Bulkconfig File Description.

   Note: Be sure to have one host entry per MEDIATION server in the bulkconfig file. Enter the hostname as ixp**NNNN-MA**, with:

   - the same **NNNN** designation (4 digits) for all the servers of the MEDIATION subsystem and the same as for the related DRS (not necessary for DRS on Standard Server)
   - the same **M** designation (1 digit, excluding "0") for all the servers for the MEDIATION subsystem and the same as for the related DRS (not necessary for DRS on Standard Server)
   - as its **A** designation (a small letter), "a" for the first server in this MEDIATION subsystem, "b" for the second server, and so on…

   Note: If a bonding interface has been configured (see section 0 Configure Bonding Interface), be sure to use the **bond0** interface (and not the usual **ethxx** interface) in the **bulkconfig** file.

Configure the server hostname

1. Enter the **platcfg** menu.

   As root, run:

   ```
   # su - platcfg
   ```

2. Select Server **Configuration** -> **Hostname**
3. Click **Edit**.
4. Enter the server hostname in the standard format: ixp***NNNN-MA***

   This name must be the same as it put in the bulkconfig file.

5. Exit the platcfg menu.

Install Mediation Server

This procedure describes how to install the Mediation Server application on the TPD platform.

Before you perform this procedure, make sure that you have the appropriate mediation server ISO file available.

Verify the /root/bulkconfig file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.

Note: Run this procedure via iLO.

Temporary customer IP assignment

This procedure provides instructions to temporary customer IP assignment to transfer the Application ISO on server during installation.

Note: This procedure is only to be used to transfer the Application ISO during installation.

Refer to Appendix A: Manual configuration of ethernet interfaces

Note: The temporary customer IP assignment is not to be executed if a bonding interface has been setup

Copy ISO

1. Copy mediation server iso to /var/TKLC/upgrade folder.

Install the application

1. From platcfg menu select **Maintenance** -> **Upgrade** -> **Initiate Upgrade**.

   When the installation process is complete, the server restarts automatically.

   Note: after the server has restarted, at login, a message asking to accept or reject the upgrade is displayed: the message can be safely ignored until the Integrate Customer Network step has been executed.

2. If the ISO file was copied to the server, then remove this file to save disk space.

   As root, run:

   ```
   # rm -f /var/TKLC/upgrade/iso_file
   ```

   where iso_file is the absolute path of the ISO image, which includes the name of the image.

Analyze the installation log

Review the installation log /var/TKLC/log/upgrade/upgrade.log for any errors.

If there are any errors, refer to Appendix E: My Oracle Support

Install JRE

Execute Install JRE 1.8

Mediation Server Post-Install Healthcheck

This procedure describes how to run the server health check after the application has been installed on the server.

1. Log in on the server that you want to analyze.
2. As cfguser, run:

   ```
   $ analyze_server.sh -p
   ```

   The script gathers the health check information from the server. A list of checks and associated results is generated. There might be steps that contain a suggested solution. Analyze the output of the script for any errors. Issues reported by this script must be resolved before any further use of this server.

   The following examples show the structure of the output, with various checks, values, suggestions, and errors.

   Example of overall output:

   ```
   08:43:58: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
   08:43:59: date: 05-17-15, hostname: ixp0907-1a
   08:43:59: TPD VERSION: 7.6.2.0.0-88.58.0
   08:44:00: IXP VERSION: [ 10.4.0.0.0-1.6.0 ]
   08:44:00: XDR BUILDERS VERSION: package TKLCxdrbuilders is not installed
   08:44:00: ------------------------------------------------
   08:44:01: Analyzing server record in /etc/hosts
   08:44:01:          Server ixp0907-1a properly reflected in /etc/hosts file
   08:44:02: Analyzing IDB state
   08:44:02:          IDB in START state
   ```

```
08:44:03: Analyzing shared memory settings
08:44:03:       Shared memory set properly
08:44:04: Analyzing IXP Licence
08:44:05:       Ixp Licence Valid
08:44:05: Analyzing mount permissions
08:44:05:       Writing enabled for pdu_1
08:44:06:       Writing enabled for pdu_2
08:44:06:       All mount permissions set properly
08:44:06: Analyzing date
08:44:07:       NTP deamon is running
08:44:07:       IP of NTP server is set
08:44:08: Checking CPU usage
08:44:08:       CPU usage check done
08:44:08: Running iaudit
08:44:10:       iaudit did not find any errors
08:44:10: Analyzing disk usage
08:44:11:       Space not exceeded
08:44:11: Analyzing JMX agent properties
08:44:12:       Instance ID of JMX agent OK
08:44:13:       IxpMbean [ application type IXP+2 ] located
08:44:13: Checking syscheck - this can take a while
08:44:17:       No active alarms
08:44:17: Checking services
08:44:17:       NFS service is running
08:44:18:       Portmap service is running
08:44:18: Analyzing bulkconfig content
08:44:19:       BulkConfig content is consistent
08:44:19: All tests passed!
08:44:19: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
```

Example of a failed test:

```
12:21:48: Analyzing IDB state
12:21:48: >>> Error: IDB is not in started state (current state X)
12:21:48: >>> Suggestion: Verify system stability and use 'prod.start' to start the product
```

Note: if the following error shows up during server analysis, it can be simply ignored, as the alarm will be cleared after Integrate Customer Network step (see below) will have been executed.

```
12:21:48: >>> Error: Alarm raised for tpdServerUpgradePendingAccept...
12:21:48: >>> Suggestion: Check /var/TKLC/log/syscheck/fail_log...
```

In any other cases, after attempting the suggested resolution, if the test fails again, then refer to Appendix E: My Oracle Support

Integrate Customer Network

This procedure describes how to integrate the mediation subsystem post-manufacturing customer network.

This procedure uses the /root/bulkconfig file as an input for the customer network integration. Before you perform this procedure, make sure you have read and are familiar with the chapter Mediation Server Bulkconfig File Description.

This procedure is run from the iLO.

1. Update the bulkconfig file
    a. Log in on the iLO of **any Mediation server** in the Mediation subsystem that you want to reconfigure.

b. Update the /root/bulkconfig file with the customer IP addresses and timezone.

c. Make entries for PDU mounts for external PDU storage in bulkconfig file.

Note: The step c. shall take care of the case where the PDU storage is done on ZFS server. The customer integration step shall automatically take into account the shared NFS mount points created on ZFS.

2. Run the customer network integration

   a. Run the mediation subsystem customer network integration script. As root, run:

   ```
   # bc_customer_integration.sh
   ```

   b. Confirm this operation. Enter

   yes.

   A prompt for the root password appears.

   c. Provide the root password. The servers reboot.

3. Run the post-integration settings

   Note: The mediation server has new IP address. The previous addresses are no longer accessible.

   a. Run post-integration settings. As root, run:

   ```
   # bc_customer_integration.sh --post
   ```

   A prompt for the root and cfguser passwords appears.

   Note: The key exchange operation is part of this script.

   b. Provide the appropriate passwords.

   When the script is complete, check the terminal output for any errors. If the error occurs, refer to Appendix E: My Oracle Support

Add Mediation Subsystem to CCM

This procedure describes how to add the Mediation subsystem to the CCM on Management server. This procedure is performed through the NSP application interface.

For an estimated time for this procedure, refer to the mediation subsystem overview flowchart.

In this release due to various security enhancements, the generation of oracle wallet and its sync to each of the server in the sub-system is mandatory. The wallet generation and syncing shall be required on every new site/sub-system creation. Refer to Appendix Modify Wallet Password

Note: a pool of DRS (it can be one single DRS) must already have been declared in CCM. A pool of DRS cannot be the primary xDR storage of several mediation subsystems (the primary xDR storage is the DRS pool that is selected when the mediation subsystem is declared in CCM).

1. Sync Database Credentials

   Execute procedure in Appendix: Sync Database Credentials

   If DRS present in the site is already added and integrated with the CCM then above procedure should be sufficient. However if DRS is not integrated into CCM then it is must to execute procedure in Appendix Modify Database Password, however the user can keep the new password same as old one. The step is just needed to create DRS credentials in the wallet and sync to the mediation servers present in the sub-system.

2. Log in to the NSP and open Centralized Configuration (CCM)
    a. Log in to the NSP application interface as tekelec using the Management Server server IP address
    b. Open the Centralized Configuration application.
    c. Select Equipment Registry.
3. Configure the new site

    Note: Configure new site only if earlier created site does not exists.
    a. Right-click the Sites list and select Add to enter new site configuration.
    b. Type the Site name and Description and click Add.
4. Add the mediation subsystem to the site
    a. Navigate to Sites.
    b. Right-click IXP and select Add to enter the mediation subsystem configuration.
    c. Type values for the following fields:
        - Mediation subsystem name in **Subsystem Name**
        - Dedicated IP address for the mediation subsystem in **VIP Address.**

            Note: The Virtual IP (VIP) Address is an actual IP address in the same subsystem subnet that is not physically used by any other server or equipment. The subsystem is treated by Management Server as a cluster accessible from Management Server through this IP address.
        - Add IP address of all mediation servers
    d. Click Add.
    e. Verify that all of the added servers are listed in the Locations list.
    f. Select the DRS pool to use as primary xDR storage.
    g. Click Create.

        Information is synchronized from the mediation servers to the Management Server.

5. Apply the configuration changes
    a. Navigate to **Mediation** tab.
    b. In the left-hand menu, open **Sites**, open the site on which the Mediation subsystem has been created, and open IXP and right-click the Mediation subsystem name.
    c. Select **Apply changes…** and click **Next**, **Next**, **Apply changes**
    d. Confirm by clicking **OK**
    e. Click **Done** when the changes have been applied

Note: "Unable to update or create capacity management session" warning must be ignored during Apply Change.

Install xDR Builders

This procedure describes how to trigger the xDR Builders installation on the Mediation subsystem from the CCM.

1. Log in on the Management Server Admin server and insert the xDR DVD/CD or copy the ISO file at /var/TKLC/upgrade, if it exists. If not then create it.

Note: Don't copy the builder ISO at root directory.

a. Open a terminal window and log in on the Management Server Admin server.

b. Insert the xDR Builders DVD/CD or copy the xDR Builder ISO file to the Management Server Admin server.

2. Run the install script

a. As root, run:

```
# cd /opt/nsp/scripts/oracle/cmd
# ./install_builder.sh
```

The following prompt appears:

Please enter path to Builder ISO [/media/cdrom]:

b. Enter the appropriate response based on the media used:

- For a DVD/CD, press **Enter.**
- For an ISO file, enter the exact path including the ISO file name.

c. Wait until the installation is complete.

Note: the script may ask password for oracle user many times.

3. Verify the ISO installation on Management Server

a. Open a web browser and log in as TklcSrv on the management server application interface.

b. Open the **Upgrade Utility**.

c. Click **Manage Builder Rpm** in the left tree.

A list of xDR Builder RPMs appears. The ISO file installed in the previous step is on this list, with a state **Not Uploaded.**

4. Upload Builders RPM

a. Select the desired xDR Builder RPM with the **Not Uploaded** state and click **Upload**. A confirmation window appears.

b. Click **Continue** to continue the RPM upload.

c. If the upload is successful, then the RPM state changes to **Uploaded.**

d. In case the RPM upload fails, then the state of will change back to "Not Uploaded" or "Query/Filter Upgrade Failed".

- If the builder RPM upload fails in creating new builder and dictionaries then the state is "Not Uploaded", after failure. At this state, this step can be repeated once the failure issues are resolved.
- If the builder RPM upload fails in upgrading the configurations (Query/xDR filter) then the state is "Query/Filter Upgrade Failed" after failure.

5. Upgrade Queries and Filters

In case the state of the RPM is "Query/Filter Upgrade Failed", then only configurations (Query/xDR filter) are required to be upgraded. Below are steps for the same

a. Mark the requested builder RPM with the “Query/Filter Upgrade Failed” state and press "Upgrade Queries and Filters” button in the toolbar.
b. A dialog box will appear. Click on Continue to continue the upgrade.
c. After the successful upload the RPM state will change to **Uploaded**

6. Associate the xDR Builders RPM with the Mediation subsystem

   a. Click **View Builder RPM Status** in the left tree. A list of the Mediation subsystems appears.

   b. Select one or more Mediation subsystems and click **Associate RPM Package**. A list of Builder RPMs that are uploaded in Management Server appears.

   c. Select the appropriate xDR Builder RPM and click **Associate**.

   If the association is successful, then the list of the subsystems is updated. The **RPM Name** column contains the new RPM package name and **Association Status** is marked as **OK.** If the association fails, refer to Appendix E: My Oracle Support

7. Apply the configuration to the Mediation subsystem

   a. Logout from TklcSrv and login with any other user with sufficient privilege for Centralized Configuration application

   b. Open the **Centralized Configuration** application.

   c. Navigate to **Mediation**.

   d. Open **Sites** and open the site; then, open **IXP**.

   e. Right-click the subsystem and select **Apply changes...**.

   f. Click **Next.**

   g. Click **Apply Changes.**

      WARNING: ***Not as TklcSrv user***.

   h. When change is complete, verify there are no errors on the result page.

8. Install the xDR Builders RPM on Mediation Server

   a. Return to the main page of the NSP application interface, log in as TklcSrv.

   b. Open the **Upgrade Utility**.

   c. Click **View Builder RPM Status** in the left tree.

      The available MEDIATION subsystem with their respective RPM Associate Status and Install Status appears.

   d. Before initiating the builder installation, make sure the **Builder RPM** that you want to install on the MEDIATION subsystem is associated with the MEDIATION subsystem as indicated by **RPM Name** column and **Association Status** marked as **OK**. Also, **Install Status** should contain either - or **No Started**.

   e. Select one or more Mediation subsystems and click **Install RPM Package**. If the installation is successful, the **Install status** changes to **OK**. If the installation fails, refer to Appendix E: My Oracle Support

Capacity Management KPIs installation

Capacity Management is a statistical session is generated with a dedicated xDR builder.

It provides very detailed self-surveillance data which can be better analyzed after selection and aggregation.

Derived statistical data are produced in real time (periodicity at the minute, quarter of hour and hour). These statistical results are stored as regular xDR, which allows to manage this with standard Performance Intelligence Center tools (such as Troubleshooting or Dashboard Application).

They globally provide system activity information in real time and an historical, traffic volume and verify the accuracy according to licenses.

Standard KPI configurations are provided and need mandatory installation steps. In addition optional customized KPI configurations could be added for more perspectives.

Installation Procedures for Capacity Management standard KPIs

This procedure describes how to deploy all needed elements for Performance Intelligence Center system monitoring. This procedure is essential for license controls and this deployment is NOT optional.

1. Capacity Management statistical session deployment
    a. All elements such as dedicated streams and DataFlows for this statistical session are automatically created as part of system deployment.
    Naming convention makes that needed elements will contain *CapacityManagement* in the name (generally as suffix).
    b. Each time a new equipment such as Mediation or Acquisition server will be added to the system, it will be taken into account by CCM to create all new needed *CapacityManagement* elements. This mechanism will be done by a check at each configuration changes.
    c. You must check whether these elements have been correctly deployed or not (by using CCM and verifying presence or not of dedicated streams and DFP).
    If not, please contact Support team in order to have the needed elements deployed for further usage of *Capacity Management*.
2. KPI templates deployment
    a. A set of KPI templates is provided.

    Refer to chapter **Capacity Management Good Practices** in 10.4.0 Maintenance Guide

    3 configurations must be deployed (no automatic feature for this operation):

    - **PIC_UsageStat_Mn**: applied on *CapacityManagement*; provides consolidation / conversion of input Mbps for probed acquisition (PMF), integrated acquisition (IMF) and mediation (MEDIATION) over 1 mn. To apply on the basic statistical session *CapacityManagement* which is part of the standard deployment.
    - **PIC_UsageStat**: applied on *PIC_UsageStat_Mn* result stat session; Agregation of PIC_UsageStat_Mn results over 15 minutes. Provides average, minimum, maximum throughput. To apply on the *PIC_UsageStats_Mn* statistical session (generated from the KPI configuration template **PIC_UsageStat_Mn**).
    - **PIC_ActivityStat**: applied on *CapacityManagement*; Aggregation of key output data flows over 15 minutes, per destination for acquisition server and per final XB for mediation server in Kbps and

efficiency. To apply on the basic statistical session *CapacityManagement* which is part of the standard deployment.

The configurations will have to be saved as text files before being imported into KPI application, on Management Server. Refer to KPI user guide to learn how to import configurations and apply them to sessions.

b. Activate the configurations

c. Check the results: the statistical sessions must be created and should contain results. After one minute for *PIC_UsageStats* and after end of next quarter for the 2 others.

For deeper usages of *Capacity Management* Refer to the dedicated document (e.g. MEDIATION and Acquisition Server troubleshooting guides).

Mediation Subsystem Healthcheck

See procedure in Appendix Mediation Subsystem Healthcheck

Mediation Server Post-Integration Configuration

This section contains various optional post-integration configuration procedures.

CSV streaming feeds

That procedure is to be followed to integrate a CSV server into a MEDIATION subsystem; such a server is used by the CSV streaming feed feature to store CSV files on a server that is not part of a MEDIATION subsystem.

Note: For the CSV streaming feed feature, instead of using a dedicated server provided by the customer, it is possible to use a PDU server which is part of the current MEDIATION subsystem or which is part of another MEDIATION subsystem (as long as all the servers are in the same LAN).

Note: The following procedures describe how to setup shared directories using the NFS v3 protocol; it may be possible to use NFS v4, but the commands to execute are not described here (you should refer to linux and NFS documentation to learn how to use NFS v4 protocol).

1. Configure the shared directory on the sharing server

   a. Select an existing directory or already mounted local file system in which the exported files will be stored.

      Note: Be sure the shared directory has read/write/execute access rights for MEDIATION’s cfguser user. If the user cfguser also exists on the sharing server, with the same UID as on the MEDIATION servers, create the shared directory as cfguser (or mount the local file system in a directory owned by cfguser); in any other case, set RWX access rights on the shared directory for everybody.

   b. Update the exports file. As root, execute:

      If the server uses a versioning system like rcstool, first check out the file:

      ```
      # rcstool co /etc/exports
      ```

      Edit /etc/exports and add this line (<path_to_share> is the directory or path to file system to share, <ip_ixp_export> is the IP address of an MEDIATION server); add as many lines as MEDIATION servers that will remotely access this shared directory

      <*path_to_share*> <*ip ixp export*>(rw,sync,anonuid=-1)

If needed, check in the file:

```
# rcstool ci /etc/exports
```

c. Restart the NFS services. As root execute:

```
# chkconfig --levels 345 nfs on
# service rpcbind restart
# service nfs restart
```

2. Mount the shared directory on MEDIATION side

   Note: These steps are to be executed on each MEDIATION server that will remotely access the shared directory of the sharing server.

   a. Create the mount point. As root, execute:

   ```
   # mkdir /var/TKLC/ixp/StoreExport
   # chown cfguser:cfg /var/TKLC/ixp/StoreExport
   ```

   b. Update the fstab file. As root, execute:

   ```
   # rcstool co /etc/fstab
   ```

   Edit /etc/fstab and add this line (<ip_server_nfs> is the IP address of the sharing server)

   <*ip server nfs*>:<*path_to_share*> /var/TKLC/ixp/StoreExport nfs rw,rsize=32768,wsize=32768,soft 0 0

   ```
   # rcstool ci /etc/fstab
   # mount --all
   ```

   c. Restart the NFS services. As root execute:

   ```
   # chkconfig --levels 345 nfs on
   # service rpcbind restart
   # service nfs restart
   ```

Note: The firewall must be disabled on the shared CSV server. If the CSV server is maintained by Oracle(Tekelec) then following steps must be performed to disable the firewall as root user:

```
# chkconfig  --levels 345 iptables off
# service iptables stop
```

If the CSV server is not maintained by Oracle then firewall must be disabled or configured to allow the nfs connections.

Configure Production Network (optional)

Execute the procedures defined in Configure Production Interface

12. VIRTUAL CUSTOMIZED PACKAGE

A single server can host multiple Performance Intelligence Center components by virtualizing each one; the number of virtualized components depends on the level/type of traffic to monitor regarding the performance expectation.

Hardware:

It is recommended to use the hardware as specified in our Hardware Installation Guidelines document. Other servers may be tried under the customer or partner responsibility. The hypervisor installation, VM configuration, Virtual networking configuration as well as the Performance Intelligence Center installation shall be done by the partner or customer.

Performances:

In general, performances are expected to be lower for virtual environment due the presence of another software layer. Therefore it is advised to monitor the selected system during a soak period to ensure it will manage properly the expected traffic.

Virtualization option by component:

- Management Server runs in a Weblogic domain with an Oracle database. Documentation is provided for deployment on a physical server. Partner or customer is free to take ownership and provide a virtual environment that is compatible with those software tools. Documented Installation steps will require adaptation.
- Probed Acquisition, OCDSR Integrated Acquisition, Mediation can be virtualized.
- The database records storage (DR storage) and flat file storage, NFS (PDU storage) can be customer provided, in that case virtualization is possible. If Oracle is to provide the storage then it is not virtualized.
- EAGLE integrated acquisition can be virtualized with the help of KVM hypervisor and openVswitch, however the switch between Eagle and integrated acquisition server is still physical. It is still possible to use E5-APP-B card in the EAGLE for the integrated acquisition when the traffic figures are compatible with this choice.

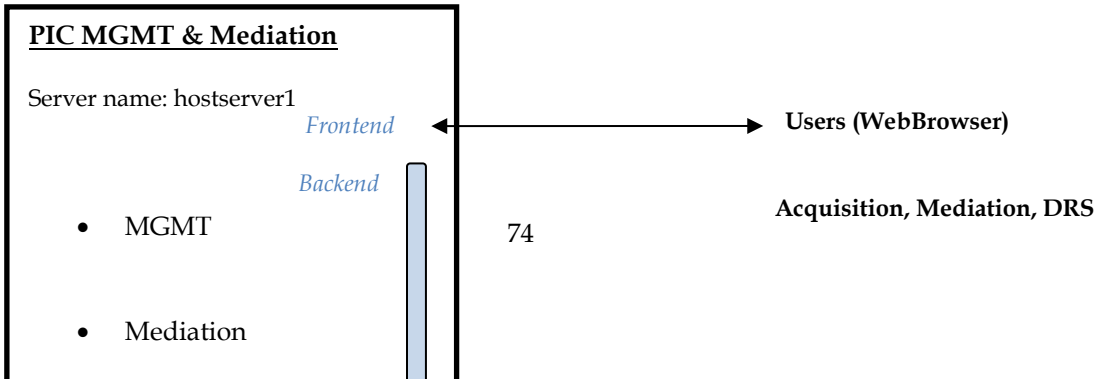
Support:

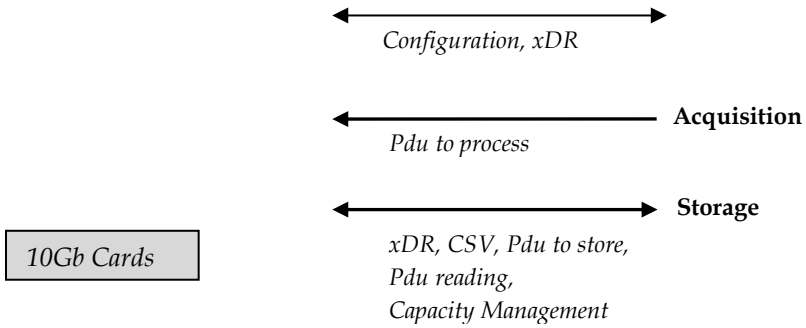
Virtualized system setup and maintenance, including security fixes, of this environment is under the responsibility of the partner or customer. Oracle will provide support on the Performance Intelligence Center software. It shall be noted that problem solving may be delayed in case of doubt of the problem origin: Performance Intelligence Center software or virtual environment.

The supported virtualization configurations are mentioned below:

1. **Configuration 1**: All PIC components except integrated acquisition on the same server (Prepackaged DSR Monitoring):
   - 1 MGMT server,
   - Up to 3 Mediation servers,
   - 1 Probed Acquisition server, if the appropriate cards for the traffic capture are physically installed in the server.

Example of Configuration 1:





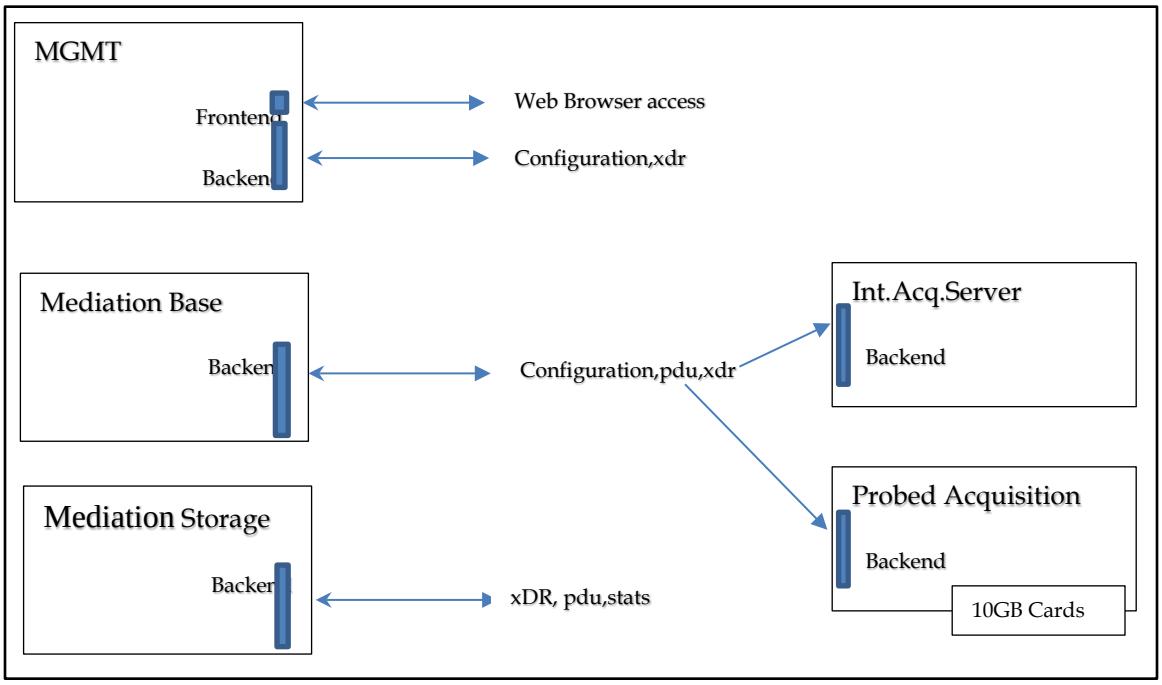
Function	vCPU Minimum / recommended	Minimum RAM	HDD Minimum / recommended	Configuration
Hypervisor	2	4 GB	200 GB	This disk volume is what remains on the host
Management	2 / 8	60 GB	550 GB / 2 TB *For 550GB:* *(150 GB MGMT, 400 GB oracle, 100 Backup).*	No. users = 1 to 5 (subject to licensing condition) Capacity Management Session, Alarms & Logs retention must be configured to 5 days, at most
Mediation	4 / 8	16 GB	64 GB	
Acquisition	4 / 8	16 GB	64 GB	For good performance, refer to pre-package Acquisition

Table 2: Ressources requirement for Performance Intelligence Center Virtual Machines

For the detailed installation of such configuration 1, Refer to the chapter **Chapter 13:** Prepackaged DSR Monitoring.

2. **Configuration 2**: One guest per SunX7-2 Host:

Example of Configuration 2



Function	vCPU Minimum / recommended	Minimum RAM	HDD Minimum / recommended	Configuration
Hypervisor	2	4 GB	100 GB	This disk volume is what remains on the host
Management	Remaining vCPUS = 94	Remaining memory=260GB	Internal Disk= remaining space (800 GB) External Disks should be used for the ASM disks	Backup partition of 100 GB can be created on the system disk.
Mediation	Remaining vCPUS = 94	Remaining memory=260GB	BASE, Internal Disk=remaining 800GB External Disks should be used for the PDU	All the available external disks should be considered for ASM disks for xDR storage. In case of PDU storage external disks

			and xDR storage.	should be considered for NFS storage.
Acquisition	Remaining vCPUS = 94	Remaining memory=260GB	Internal Disk=remaining 800GB	10GB cards should be made pass through in Probed server.

Table 3: Hardware Resources for PIC VM in one VM per host configuration

For the detailed installation of such configuration 2, Refer to the chapter **Virtual Installation on SUN X7-2**.

13. PREPACKAGED DSR MONITORING

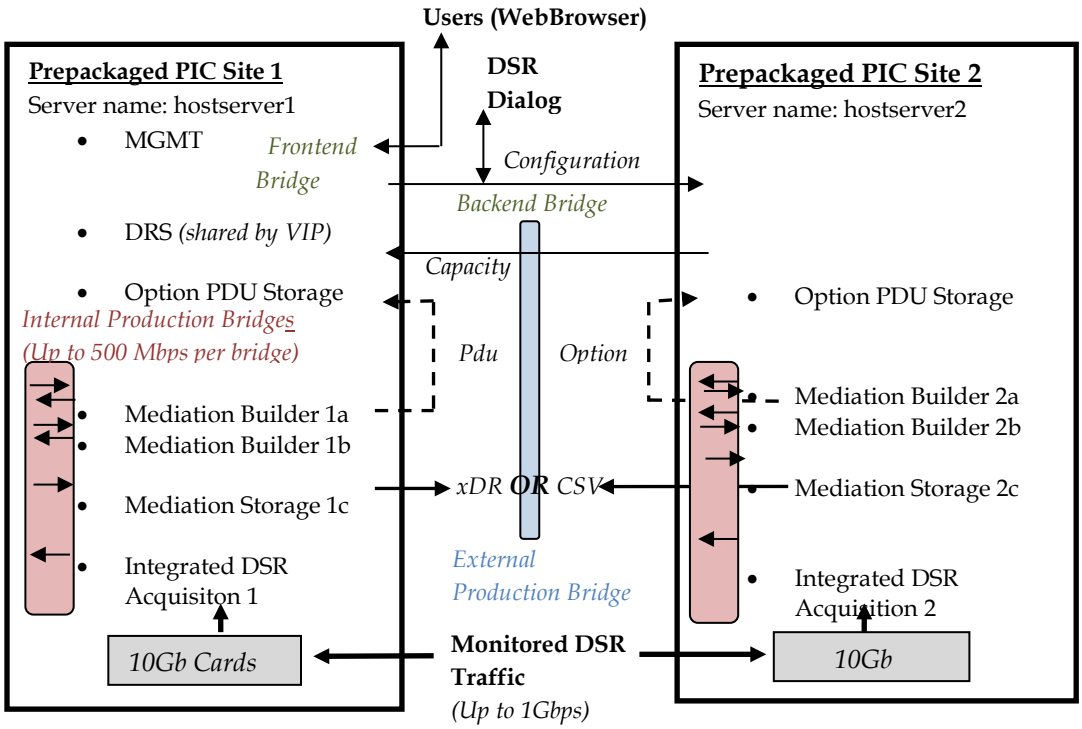
Configuration Overview

This configuration is targeted for DSR Monitoring, for Troubleshooting and/or Accounting on hardware as specified in our Hardware Installation Guidelines document.

DSR is the "Diameter Signaling Router provided by Oracle.

There is one Acquisition/Mediation server per DSR site. One of them is also hosting Management server and a small DRS for the Capacity Management feature. The number of users is limited as per licensing rules.

Both servers are receiving the double of the Network traffic in case of DSR failover. In other words, most of the time, each server is running at half capacity.



For better performance, it is recommended to use two Mediation Virtual Machine (VM) for the Builder processing versus too many DataFlow processing in one VM.

It is also recommended to dedicate a Mediation VM for the Storage processing. KPI processing is not proposed in this configuration for performance reason.

The configuration can be tuned for low traffic but with the minimum of configuration per VM defined in the document Hardware Guidelines docID E66862 (see chapter **Error! Reference source not found.**).

We suggest to follow the proposed configuration, tuned for 1 Gbps capacity, versus reducing the number of VMs or vCPU for some lower traffic and being obliged to modify in case of traffic increase. You have to be aware that changing the configuration could interrupt the DSR Monitoring during all the time of the modifications.

In case of Accounting without Troubleshooting, there is no need of External Data record Storage and no need of PDU Storage.

Two servers must be installed for OCDSR Integrated Acquisition , one on each DSR site.

Two vSwitch bridges are created for Acquisition to the Mediation Builder; another vSwitch bridge is created for the two Mediation Builder to the Mediation Storage.

The hardware of the prepackaged solution allows this configuration parameters:

Function	vCPU	Minimum RAM	Minimum HDD	Configuration
Hypervisor	2	4	200 GB (*)	(*) This disk volume is what remains on the host
Management, DRS, PDU Storage	2	60 GB	650 GB (150 GB MGMT, 400 GB oracle, 100 Backup). 3.6 TB for PDU storage	No. users = 1 to 5 (subject to licensing condition) Capacity Management Session, Alarms & Logs retention must be configured to 5 days, at most Option: PDU Storage for the "Troubleshooting Use Case"
Acquisition	8	16 GB	64 GB	Load Balancing for 12 DFPs.
Mediation-1a	8	16 GB	64 GB	6 DFPs Builder
Mediation-1b	8	16 GB	64 GB	6 DFPs Builder
Mediation-1c	8	16 GB	64 GB	**Accounting Use Case**: 12 DFPs CSV Store **Troubleshooting Use Case**: 12 DFPs xDR Store

Table 4: Resources Performance Intelligence Center Virtual Machine for DSR Monitoring

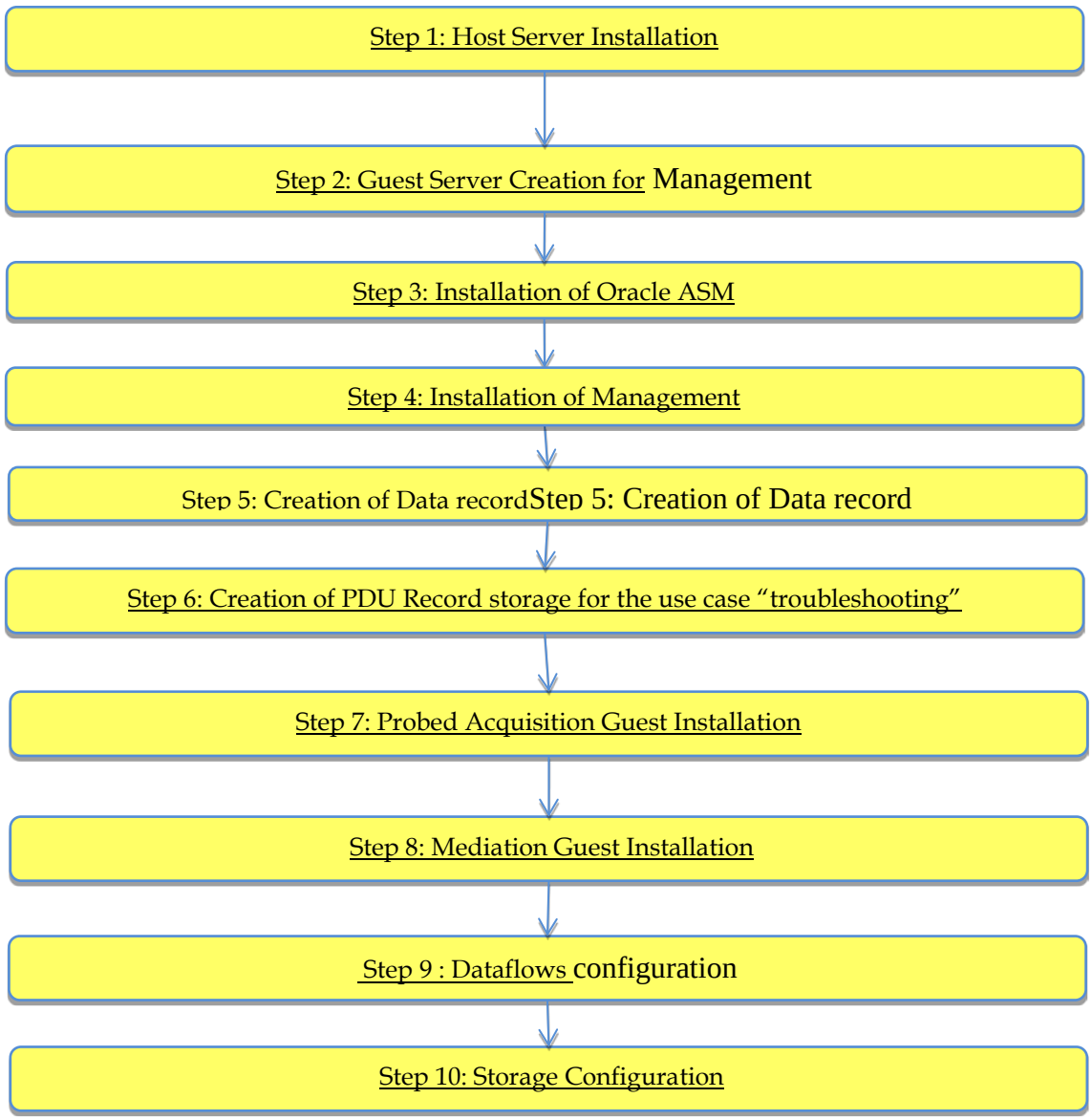
Configuration Steps

This chapter describes the steps to follow in a scrupulous manner to achieve the configuration in optimized timing.

Note: KVM or VmWare can be used. Examples of commands are provided for KVM.

See the detailed schema provided in the next chapter.

Figure 4. High level Pre-Package installation



Caution: This installation requires a good skill in virtualization environment.

Step 1: Host Server Installation

This step must be done on Server 1 and 2.

1. Installation of Oracle Linux

   Refer to the Chapter Oracle Linux on Third-Party Server Installation

   With the following Base environment option:

a. Choose Base environment “Server with GUI” and Add-Ons "Virtualization Client", “Virtualization Hypervisor” and "Virtualization Tools”.

b. The “Manual Partitioning” must be adapted to the available disk space

   Refer to System Partitioning Recommendation

c. The network shall not be configured yet (this will be done during the bridges creation)

(2) NTP Configuration

NTP must be configured on the host server as a reference for all internal VMs.

Refer to section How to configure NTP.

(3) Enable PCI Pass through mode for the 10GB Acquisition card

This mode is required when 10 GB Ethernet links are to be directly handled by a Probed Acquisition guest. Execute the following procedure to enable the PCI pass through mode:

Verify and update /etc/grub2-efi.cfg

a. open a ssh console on the host as root
b. edit the file */etc/grub2-efi.cfg*
c. look for all the lines having “linuxefi /vmlinuz-x.y.x”, where x.y.z is the kernel image version.
   For example:
   linuxefi /vmlinuz-4.1.12-94.3.9.el7uek.x86_64 root=/dev/mapper/ol-root ro crashkernel=auto rd.lvm.lv=ol/root rd.lvm.lv=ol/swap rhgb quiet LANG=en_US.UTF-8

   Modify the above line with following:
   linuxefi /vmlinuz-4.1.12-94.3.9.el7uek.x86_64 root=/dev/mapper/ol-root ro console=ttyS0,115200n8 console=tty0 intel_iommu=on

   This should be done for all such instances.
d. save the file

Enable intel_iommu parameter in grub configuration

a. open a ssh console on the host as root
b. edit the file /etc/default/grub
c. look for a line starting with the GRUB_CMDLINE_LINUX keyword
d. at the end of that line, before the closing quotes, add a space character and append intel_iommu=on
e. save the file
f. run the command to update the bootloader:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

g. reboot the host

(4) Identify and detach the 10Gb Ethernet links

If a Probed Acquisition guest is planned to control the 10Gb Ethernet links, those links need to be identified by their bus, slot and function. Proceed as follows:

a. open a ssh console on the host as root
b. use the lspci command in conjunction with a grep command to identify the 10Gb Ethernet links
   Example:

```
# lspci|grep SFP
```

```
03:00.0 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
03:00.1 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
13:00.0 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
13:00.1 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
```

c. take note of the bus, slot and function of each 10 Gb Ethernet link. In the previous example, for the 1st link, the bus is 03, the slot is 00 and the function is 0.

Detaching the 10Gb Ethernet link devices is a prerequisite to attach the links in a dedicated guest. Proceed as follows to detach a device:

a. open a ssh console on the host as root
b. use the virsh command in conjunction with a grep command to get the device ID. For the 1st Ethernet link of the previous example, use the following command, where bus, slot and function are used as the grep argument:

```
# virsh nodedev-list|grep 'pci.*03_00_0$'
pci_0000_03_00_0
```

c. then, use the previously found ID to detach the device with the following command:

```
# virsh nodedev-detach pci_0000_03_00_0
Device pci_0000_03_00_0 detached
```

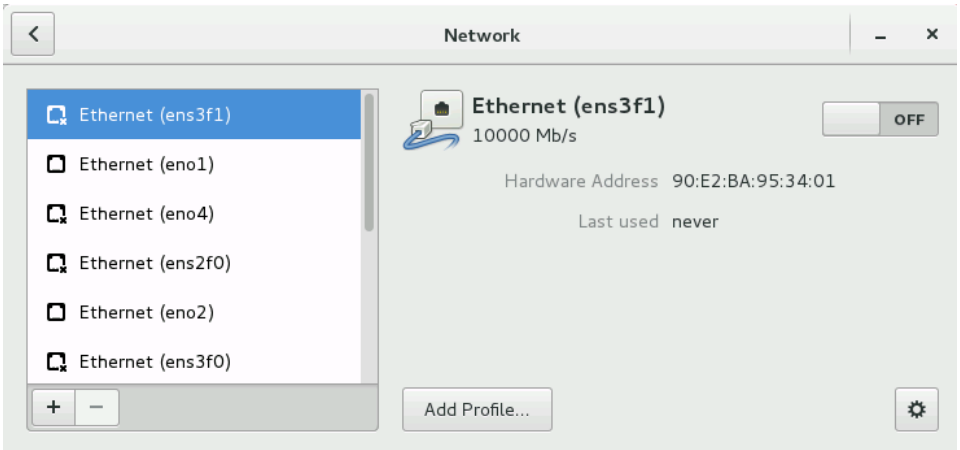
d. repeat both previous steps to detach the remaining devices

(5) Network configuration help for the creation of:

- Backend bridge (DRS access for Capacity Manangement, when not installed on an external storage)
- Frontend bridge (MGMT access), when not installed on a dedicated server
- 3 Internal Production bridges for high performance between VM Acquisition & Mediations
- External Production bridge (CSV, xDR, PDU)

Follow these recommendations for the prepackaged solution.

a. **Backend** bridge
    - In order to give access to the “Capacity management” DRS from the Mediation of the second server,you need to add a bridge for the backend IP address. Make sure that no route is configured for this bridge (DEFROUTE=no).
    - Through All Settings/Network, the following windows is open:



- With the "+" button you can add a Network Connection and select "Bridge".
- Give a name to the bridge, e.g "**Backend**" and Add a Bridged Connections, choose "Ethernet", select the appropriate "Device" and give an IP Address

b. **Frontend** bridge

- Proceed as for the Backend bridge but with DEFROUTE=yes

c. Internal **Production** bridges

- These 3 bridges, named **Prod1**, **Prod2** and **Prod3**, allow **internal** server communication between the VMs. Add no Bridged Connections.
- Give a name to the bridge, e.g "**Prod1**", give an IP Address and set DEFROUTE=no

d. External **Production** bridge

- This bridge, named **Storage**, allows **external** server communication for CSV,xDR and PDU
- Proceed as for the Backend bridge but with DEFROUTE=no

Step 2: Guest Server Creation for Management

Management Server must be installed only one time for the Performance Intelligence Center system to manage.

Management Guest Creation

1. Creation of the Management server guest

```
# virt-install --virt-type kvm --hvm --connect qemu:///system --network bridge=Backend,model=virtio --network bridge=Frontend,model=virtio --network bridge=Prod3,model=e1000 --network bridge=Storage,model=e1000 --cdrom /var/ORCL/V74844-01.iso --disk path=/var/vm_server/MGMT.disk,size=150,sparse=no,bus=ide --name MGMT --autostart --boot cdrom,hd --ram 64512 --vcpus 2 --graphics vnc --os-variant rhel6
```

2. Installation of Oracle Linux
   Refer to the document Oracle linux on Third-Party Server Installation

   a. Hostname configuration
      Configure in /etc/hosts file the IP address which contain the backend IP address
   b. Default Linux installation tuning
      System Partitioning Recommendation

MGMT Backup: It is possible to create space for the Backup, like 100GB but it is recommended to store the backup on one other server using nfs share like done for PDU. This other server can be the server of prepackaged of the site 2.

3. Define a disk with minimum 100GB and allocate all for the "NSP daily backup" partition.

Management Guest OS reinstallation

In order to reinstall the OS, the ISO file of the Oracle linux is needed on the host

Use this procedure when the OS is to be reinstalled on an existing guest (the previous section explains how to create a new guest):

1. Open an X terminal as root
2. Reinstall the OS on the existing guess:
   - open the guest's console: virt-viewer <*vm_name*> &
   - find the target name of the CDROM device (get the value in the Target column, on the cdrom line): virsh domblklist <*vm_name*> --details
   - attach the OS disk: virsh attach-disk <*vm_name*> <*tpd_iso_file*> <*target*> --type cdrom --mode readonly
   - reboot the guest: virsh reboot <*vm_name*>. **Don't forget to check the reboot order.**

   where
   - <*vm_name*> is the name of the VM
   - <*tpd_iso_file*> is the full path and name of the TPD ISO file
   - <*target*> is the target name of the CDROM device on the VM

   Example:

```
# virt-viewer MGMT &
# virsh domblklist MGMT --details
Type         Device       Target       Source
-------------------------------------------------
file         disk         hda          /var/vm_server/MGMT.disk
block        cdrom        hdb          -
file         disk         hdc          /var/lib/libvirt/images/MGMT.qcow2
block        disk         hdd          /dev/sdb1
# virsh attach-disk /var/ORCL/V74844-01.iso hdb --type cdrom --mode readonly
# virsh reboot MGMT
```

Note: after the server has rebooted, it might be possible that the Oracle linux ISO has not been ejected. In this case, the ISO has to be manually ejected and the server restarted. Example:

```
# virsh destroy MGMT
# virsh change-media MGMT hdb --eject
# virsh start MGMT
```

3. Installation of Oracle Linux
   Refer to the document Oracle linux on Third-Party Server Installation

   a. Hostname configuration
      Configure in /etc/hosts file the IP address which contain the backend IP address
   b. Default Linux installation tuning

System Partitioning Recommendation

MGMT Backup: It is possible to create space for the Backup, like 100GB but it is recommended to store the backup on one other server using nfs share like done for PDU. This other server can be the server of prepackaged of the site 2.

4. Define a disk with minimum 100GB and allocate all for the “NSP daily backup” partition.

Step 3: Installation of Oracle ASM

This step must be done on the server hosting the Management Server and/or a DRS for Capacity management.

Refer to the chapter Oracle ASM and database on Third-Party Server Installation

Define a disk with minimum 400GB and allocate all for oracle ASM.

Step 4: Installation of Management Server

To install the application on the guest, refer to Chapter 8 for Installation of Management Server on Third-Party Server.

At the end of installation:

1. Check nsp and jmx services:

```
# systemctl status nspservice
# service jmxd status
```

If they aren’t running, please start services.

```
# systemctl start nspservice
# service jmxd start
```

2. Configure log storage duration, in an sqlplus command:

```
> update cor_system_config set CONFIGURATION_VALUE=’5’ where CONFIGURATION_NAME in
(‘ALR_PURGE_DAYS_THRESHOLD’,’LOG_PURGE_AUDIT_DEPTH’,’LOG_PURGE_DEPTH’);
> commit;
```

Step 5: Creation of Data record

1. Installation of the Data Record for Capacity Management.
   This DRS is requested to be installed on this server when there is no external DRS available.
   On Management server, refer to the Data WhareHouse Server (DWS) on Third-Party Server Installation for Performance Intelligence Center.
   The IXP database is created with a smallest size:

```
CREATE DATABASE IXP
    CONTROLFILE REUSE
    LOGFILE GROUP 1 ('+DATA') SIZE 20G,
        GROUP 2 ('+DATA') SIZE 20G,
        GROUP 3 ('+DATA') SIZE 20G,
        GROUP 4 ('+DATA') SIZE 20G
    DATAFILE '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
        '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G
        EXTENT MANAGEMENT LOCAL
```

```
SYSAUX DATAFILE '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
    '+DATA' SIZE 500M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G
DEFAULT TEMPORARY TABLESPACE temp
    TEMPFILE '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 8G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 8G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 8G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 8G
        EXTENT MANAGEMENT LOCAL UNIFORM SIZE 10M
UNDO TABLESPACE undo
    DATAFILE '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G,
        '+DATA' SIZE 100M REUSE AUTOEXTEND ON NEXT 100M MAXSIZE 16G
CHARACTER SET AL32UTF8
SET TIME_ZONE = 'America/New_York';
```

2. Add the Data Record storage on the Management Application Interface
   Refer to chapter Add Data Record Storage in the document
   Centralized Configuration Manager Administrator Guide,
3. Define a Virtual IP Address on the Data Record Storage

   To do this action on the Data Record storage from the first server, in order to benefit of the Capacity Management feature for the second server.

   Define a virtual IP address:

```
# ip addr add <IP> dev <DEV>
```

   where <IP> is the virtual IP address and <DEV> is the network device name (eg: eth0, eno1678032…)

Step 6: Creation of PDU Record storage for the use case “troubleshooting”

When there is dedicated disks for the PDU Record storage, refer to the chapter Packet Data Unit Storage on Third-Party Server Installation

For example, with 6 disks of 1.2 TB in RAID configuration, define a disk with minimum 3TB and allocate all for PDU writing (3.6 TB of space Max in this example).

Step 7: Probed Acquisition Guest Installation

This step must be done on each server hosting a Probed Acquisition.

In order to create the Probed Acquisition guest or to reinstall the OS, the ISO file of the TPD used for IPM is needed on the host.

Note: the following procedures are to be executed from the graphical desktop of the host.

Probed Guest Creation

Use this procedure when a new guest is to be created (the next section explains how to reinstall the OS on an existing guest):

A command line, ready to used, is provided for KVM environment.

1. Open an X terminal as root
2. The following arguments are to be provided to the virt-install command:
   - Virtualization mode: --virt-type kvm --hvm --connect qemu:///system
   - Network interfaces (keep the order):
     - Management: --network bridge=<*mgmt_br*>,model=virtio
     - Production: --network bridge=<*prod_br*>,model=e1000
       (This model because we recommend to distribute evenly the model of interface between virtio and e1000)
     - Capture (use anyone of the 2 options, multiple times if required, and once for each capture interface):
       - 10Gb Ethernet links detached from host: --host-device <*pci_device_id*>,rom_bar=off
       - Non-detached links: --network type=direct,source=<*phys_itf*>,source_mode=passthrough,model=virtio
   - Boot order: --boot cdrom,hd
   - CD drive: --cdrom <*tpd_iso_file*>
   - Disk: --disk path=<*disk_file*>,size=<*disk_size*>,sparse=no,bus=ide
   - VM name: --name <*vm_name*>
   - RAM: --memory <*ram_size*>
   - CPU: --vcpus <*cpu_count*>,cpuset=<*cpu_set*>
   - Display: --graphics vnc
   - VM optimization: --os-variant rhel6

   where
   - <*mgmt_br*> is the name of the network bridge used for the management network
   - <*prod_br*> is the name of the network bridge used for the production network
   - <*pci_device_id*> is the identifier (of the capture network interface) used in the virsh nodedev-detach command
   - <*phys_itf*> is the name of the network device used for the capture network
   - <*tpd_iso_file*> is the full path and name of the TPD ISO file
   - <*disk_file*> is the full path and name of the disk file (be sure to create it on a file system having enough space)
   - <*disk_size*> is the size (in GB) of the disk to create
   - <*vm_name*> is the name of the VM (preferably use letters, digits, underscores and hyphens)
   - <*ram_size*> is the size (in GB) of RAM to allocate to the VM; do not over allocate as the host itself and all of the guests will use RAM
   - <*cpu_count*> is the number of CPU to allocate to the VM; do not over allocate as the host itself and all of the guests will use CPU
   - <*cpu_set*> is the list of CPUs to assign to the VM

     Eg: --vcpus 8,cpuset=3-10 (the VM will use the physical CPU 3 to 10).

   Command for Acquisition VM (example with 2 capture interfaces 10Gb detached from host):

```
# virt-install --virt-type kvm --hvm --connect qemu:///system --network bridge=Backend,model=virtio --network bridge=Prod1,model=e1000 --network bridge=Prod2,model=e1000 --host-device pci_0000_03_00_0,rom_bar=off --host-device pci_0000_03_00_1,rom_bar=off --cdrom /var/ORCL/TPD.install-7.6.1.0.0_88.55.0-OracleLinux6.9-x86_64.iso --disk path=/var/vm_server/VM_PMF_0a.disk,size=64,sparse=no,bus=ide --name VM_PMF_0a --autostart --boot cdrom,hd --ram 16384 --vcpus 8,cpuset=3-10 --graphics vnc --os-variant rhel6
```

3. A window with the guest’s main console should pop up:

Proceed with the standard

Acquisition Subsystem installation (choose TPDnoraid console=tty0 as boot arguments); be sure to proceed with Probed Guest network right after IPM. Take also care of using the host as the NTP server.

Note: after the server has rebooted, it might be possible that the TPD ISO has not been ejected. In this case, the ISO has to be manually ejected and the server restarted. Example:

```
# virsh destroy VM_PMF_0a
# virsh change-media VM_PMF_0a hdb --eject
# virsh start VM_PMF_0a
```

4. In MGMT, in the Centralized Configuration, declare the production network Prod1 on eth05 (refer to CCM user guide, section "Adding a Production Interface to a Probed Acquisition").

Probed Guest OS reinstallation

In order to reinstall the OS, the ISO file of the TPD used for IPM is needed on the host

Use this procedure when the OS is to be reinstalled on an existing guest (the previous section explains how to create a new guest):

1. Open an X terminal as root
2. Reinstall the OS on the existing guess:
   - open the guest's console: virt-viewer <*vm_name*> &
   - find the target name of the CDROM device (get the value in the Target column, on the cdrom line): virsh domblklist <*vm_name*> --details
   - attach the OS disk: virsh attach-disk <*vm_name*> <*tpd_iso_file*> <*target*> --type cdrom --mode readonly
   - reboot the guest: virsh reboot <*vm_name*>

   where
   - <*vm_name*> is the name of the VM
   - <*tpd_iso_file*> is the full path and name of the TPD ISO file
   - <*target*> is the target name of the CDROM device on the VM

   Example:

```
# virt-viewer VM_PMF_0a &
# virsh domblklist VM_PMF_0a --details
Type         Device       Target       Source
------------------------------------------------
file         disk         hda          /var/vm_server/VM_PMF_0a.disk
block        cdrom        hdb          -
# virsh attach-disk VM_PMF_0a /var/ORCL/TPD.install-7.6.1.0.0_88.55.0-OracleLinux6.10-x86_64.iso hdb --
type cdrom --mode readonly
# virsh reboot VM_PMF_0a
```

In the guest's console, proceed with the standard

3. Acquisition Subsystem installation (choose TPDnoraid console=tty0 as boot arguments) ; be sure to proceed with Probed Guest network right after IPM. Take also care of using the host as the NTP server.
   Note: after the server has rebooted, it might be possible that the TPD ISO has not been ejected. In this case, the ISO has to be manually ejected and the server restarted. Example:

```
# virsh destroy VM_PMF_0a
# virsh change-media VM_PMF_0a hdb --eject
# virsh start VM_PMF_0a
```

Probed Guest network

Caution: During TPD installation of the virtual Probed Acquisition, the order of network declaration is modified. Go through the following tuning.

1. Take note of the mapping between bridges, MAC addresses and current device names.
   a. Get the mapping between bridges and MAC addresses from the host server, as root, with the following command:

```
# virsh domiflist <vm_name>
Interface   Type       Source     Model       MAC
-------------------------------------------------------
xxxxxx      bridge     Backend    virtio      aa:aa:aa:aa:aa:aa
xxxxxx      bridge     Prod1      e1000       bb:bb:bb:bb:bb:bb
xxxxxx      bridge     Prod2      e1000       cc:cc:cc:cc:cc:cc
```

   Note: the capture interfaces will not be listed. Their MAC addresses are only visible in the 70-persistent-files and in the ifcfg-ethX files, on the VM.
   b. Get the mapping between MAC addresses and current device names from the VM, as root, with the following command:

```
# head /sys/class/net/eth?/address
```

   Note: all the network interfaces will be listed, including capture interfaces.
   c. Using the following naming rules, prepare a reminder table to make the next steps easier.
      - Backend (MAC aa:aa:aa:aa:aa:aa) maps to eth01
      - Prod1 (MAC bb:bb:bb:bb:bb:bb) maps to eth05
      - Prod2 (MAC cc:cc:cc:cc:cc:cc) maps to eth06
      - Other production interfaces map to eth07, eth08 and eth09 (eth02, eth03 and eth04 are reserved for production interfaces that are automatically bonded as bond0)
      - MAC addresses for the capture interfaces map to eth11, eth12… up to eth99

Bridge	MAC address	Current name	New name
Backend			eth01
Prod1			eth05
Prod2			eth06
...			
Capture1			eth11
...			

2. Update the UDEV network file

   As root, on the VM, using the reminder table:
   a. Check the configuration file 70-persistent-net.rules out:

```
# rcstool co /etc/udev/rules.d/70-persistent-net.rules
```

b. Update the NAME value in the UDEV network configuration file 70-persistent-net.rules to match the new name of the devices (use vi to update the file)
c. Check the configuration file 70-persistent-net.rules in:

```
# rcstool ci /etc/udev/rules.d/70-persistent-net.rules
```

3. Update the network configuration files

As root, on the VM, repeat these steps for each network configuration file, using the reminder table:

a. Rename the configuration file ifcfg-ethN (where N is a single digit, 0 or more) to ifcfg-ethxy (where xy are the 2 digits making the new name of that network device)

```
# mv /etc/sysconfig/network-scripts/ifcfg-eth<N> /etc/sysconfig/network-scripts/ifcfg-eth<xy>
```

b. Update the DEVICE entry in the network configuration file ifcfg-ethxy to match the new name of the device; set the ONBOOT entry to no; remove a possible PERSISTENT_DHCLIENT entry (use vi to update the file)
c. Enter the network configuration file ifcfg-ethxy in the version checking tool:

```
# rcstool init /etc/sysconfig/network-scripts/ifcfg-eth<xy>
```

4. Reconfigure udev and reboot

As root, on the VM, follow the steps below:

```
# udevadm control --reload
# udevadm trigger
# reboot
```

Step 8: Mediation Guest Installation

This step must be done on Server 1 and 2.

Installation of each Mediation, refer to the chapter Mediation guest creation and after to the chapter Mediation application installation procedures.

In order to create the Mediation guest or to reinstall the OS, the ISO file of the TPD used for IPM is needed on the host.

Note: the following procedures are to be executed from the graphical desktop of the host.

Mediation Guest Creation

Use this procedure when a new guest is to be created (the next section explains how to reinstall the OS on an existing guest):

Command lines, ready to used,are provided for KVM environment.

1. Open an X terminal as root
2. The following arguments are to be provided to the virt-install command:
   - Virtualization mode: --virt-type kvm --hvm --connect qemu:///system
   - Network interfaces (keep the order):
     - Management: --network bridge=<*mgmt_br*>,model=virtio
     - Production: --network bridge=<*prod_br*>,model=virtio
   - Boot order: --boot cdrom,hd
   - CD drive: --cdrom <*tpd_iso_file*>
   - Disk: --disk path=<*disk_file*>,size=<*disk_size*>,sparse=no,bus=ide
   - VM name: --name <*vm_name*>
   - RAM: --memory <*ram_size*>
   - CPU: --vcpus <*cpu_count*>,cpuset=<*cpu_set*>

- Display: --graphics vnc
- VM optimization: --os-variant rhel6

where

- <*mgmt_br*> is the name of the network bridge used for the management network
- <*prod_br*> is the name of the network bridge used for the production network
- <*tpd_iso_file*> is the full path and name of the TPD ISO file
- <*disk_file*> is the full path and name of the disk file (be sure to create it on a file system having enough space)
- <*disk_size*> is the size (in GB) of the disk to create
- <*vm_name*> is the name of the VM (preferably use letters, digits, underscores and hyphens)
- <*ram_size*> is the size (in GB) of RAM to allocate to the VM; do not over allocate as the host itself and all of the guests will use RAM
- <*cpu_count*> is the number of CPU to allocate to the VM; do not over allocate as the host itself and all of the guests will use CPU
- <*cpu_set*> is the list of CPUs to assign to the VM

  Eg: --vcpus 8,cpuset=3-10 (the VM will use the physical CPU 3 to 10).

Linux command for first Mediation VM:

```
# virt-install --virt-type kvm --hvm --connect qemu:///system --network bridge=Backend,model=virtio --network bridge=Storage,model=virtio --network bridge=Prod1,model=e1000 --network bridge=Prod3,model=e1000 --cdrom /var/ORCL/TPD.install-7.3.0.0.0_88.54.0-OracleLinux6.9-x86_64.iso --disk path=/var/vm_server/VM_IXP_1a.disk,size=64,sparse=no,bus=ide --name VM_IXP_1a --autostart --boot cdrom,hd --ram 16384 --vcpus 8,cpuset=11-18 --graphics vnc --os-variant rhel6
```

Linux command for second Mediation VM:

```
# virt-install --virt-type kvm --hvm --connect qemu:///system --network bridge=Backend,model=virtio --network bridge=Storage,model=virtio --network bridge=Prod2,model=e1000 --network bridge=Prod3,model=e1000 --cdrom /var/ORCL/TPD.install-7.6.1.0.0_88.55.0-OracleLinux6.10-x86_64.iso --disk path=/var/vm_server/VM_IXP_1b.disk,size=64,sparse=no,bus=ide --name VM_IXP_1b --autostart --boot cdrom,hd --ram 16384 --vcpus 8,cpuset=19-26 --graphics vnc --os-variant rhel6
```

Linux command for last Mediation VM:

```
# virt-install --virt-type kvm --hvm --connect qemu:///system --network bridge=Backend,model=virtio --network bridge=Storage,model=virtio --network bridge=Prod3,model=virtio --cdrom /var/ORCL/TPD.install-7.6.1.0.0_88.55.0-OracleLinux6.10-x86_64.iso --disk path=/var/vm_server/VM_IXP_1c.disk,size=64,sparse=no,bus=ide --name VM_IXP_1c --autostart --boot cdrom,hd --ram 16384 --vcpus 8,cpuset=27-34 --graphics vnc --os-variant rhel6
```

3. A window with the guest’s main console should pop up: proceed with the standard Mediation Subsystem installation (choose TPDnoraid console=tty0 as boot arguments); be sure to proceed with Mediation Guest network right after IPM. Take also care of using the host as the NTP server.
   Note: after the server has rebooted, it might be possible that the TPD ISO has not been ejected. In this case, the ISO has to be manually ejected and the server restarted.
   Example:

```
# virsh destroy VM_IXP_1a
# virsh change-media VM_IXP_1a hdb --eject
# virsh start VM_IXP_1a
```

4. Session duration tuning
   Due to limitation of disk space, once the Mediation server is declared in MGMT, change the Capacity Management session duration to 5 days.

Mediation Guest OS reinstallation

In order to reinstall the OS, the ISO file of the TPD used for IPM is needed on the host

Use this procedure when the OS is to be reinstalled on an existing guest (the previous section explains how to create a new guest):

1. Open an X terminal as root
2. Reinstall the OS on the existing guess:
   - open the guest's console: virt-viewer <*vm_name*> &
   - find the target name of the CDROM device (get the value in the Target column, on the cdrom line): virsh domblklist <*vm_name*> --details
   - attach the OS disk: virsh attach-disk <*vm_name*> <*tpd_iso_file*> <*target*> --type cdrom --mode readonly
   - reboot the guest: virsh reboot <*vm_name*>

   where
   - <*vm_name*> is the name of the VM
   - <*tpd_iso_file*> is the full path and name of the TPD ISO file
   - <*target*> is the target name of the CDROM device on the VM

   Example:

```
# virt-viewer VM_IXP_1a &
# virsh domblklist VM_IXP_1a --details
Type            Device        Target        Source
-------------------------------------------------
file            disk          hda           /var/vm_server/VM_IXP_1a.disk
block           cdrom         hdb           -
# virsh attach-disk VM_IXP_1a /var/ORCL/TPD.install-7.6.1.0.0_88.55.0-OracleLinux6.10-x86_64.iso hdb --
type cdrom --mode readonly
# virsh reboot VM_IXP_1a
```

3. In the guest's console, proceed with the standard Mediation Subsystem installation (choose TPDnoraid console=tty0 as boot arguments) ; be sure to proceed with Mediation Guest network right after IPM. Take also care of using the host as the NTP server.

   Note: in the case of a Disaster Recovery, don't forget to set DR-BASE as the platform function in the bulkconfig file.

   Note: after the server has rebooted, it might be possible that the TPD ISO has not been ejected. In this case, the ISO has to be manually ejected and the server restarted.

   Example:

```
# virsh destroy VM_IXP_1a
# virsh change-media VM_IXP_1a hdb --eject
# virsh start VM_IXP_1a
```

Mediation Guest network

To use Prod1 and Prod2 for VM Mediation Builders and Prod3 for MediationStorage, follow these instructions:

1. Take note of the mapping between bridges, MAC addresses and current device names.

a. Get the mapping between bridges and MAC addresses from the host server, as root, with the following command:

```
# virsh domiflist <vm_name>
Interface  Type       Source     Model       MAC
-------------------------------------------------------
xxxxxx     bridge     Backend    virtio      aa:aa:aa:aa:aa:aa
xxxxxx     bridge     Prod1      e1000       bb:bb:bb:bb:bb:bb
xxxxxx     bridge     Prod2      e1000       cc:cc:cc:cc:cc:cc
xxxxxx     bridge     Prod3      e1000       dd:dd:dd:dd:dd:dd
xxxxxx     bridge     Storage    e1000       ee:ee:ee:ee:ee:ee
```

b. Get the mapping between MAC addresses and current device names from the VM, as root, with the following command:

```
# head /sys/class/net/eth?/address
```

c. Using the following naming rules, prepare a reminder table to make the next steps easier.
- Backend (MAC aa:aa:aa:aa:aa:aa) maps to eth01
- Prod1 (MAC bb:bb:bb:bb:bb:bb) maps to eth05
- Prod2 (MAC cc:cc:cc:cc:cc:cc) maps to eth06
- Prod3 (MAC dd:dd:dd:dd:dd:dd) maps to eth07
- Storage (MAC ee:ee:ee:ee:ee:ee) maps to eth08

Bridge	MAC address	Current name	New name
Backend			eth01
Prod1			eth05
Prod2			eth06
Prod3			eth07
Storage			eth08

Note: Prod1 and Prod2 network interfaces do not necessarily exist on all the Mediation servers, as these are the interfaces to connect to the Acquisition server (a Mediation server dedicated to xDR storing does not have any of those network interfaces; a Mediation server dedicated to PDU correlation has one of those network interfaces).

2. Update the UDEV network file

As root, on the VM, using the reminder table:

a. Check the configuration file 70-persistent-net.rules out:

```
# rcstool co /etc/udev/rules.d/70-persistent-net.rules
```

b. Update the NAME value in the UDEV network configuration file 70-persistent-net.rules to match the new name of the devices (use vi to update the file)

c. Check the configuration file 70-persistent-net.rules in:

```
# rcstool ci /etc/udev/rules.d/70-persistent-net.rules
```

3. Update the network configuration files

As root, on the VM, repeat these steps for each network configuration file, using the reminder table:

a. Rename the configuration file ifcfg-ethN (where N is a single digit, 0 or more) to ifcfg-ethxy (where xy are the 2 digits making the new name of that network device)

```
# mv /etc/sysconfig/network-scripts/ifcfg-eth<N> /etc/sysconfig/network-scripts/ifcfg-eth<xy>
```

b. Update the DEVICE entry in the network configuration file ifcfg-ethxy to match the new name of the device; set the ONBOOT entry to no; remove a possible PERSISTENT_DHCLIENT entry (use vi to update the file)

c. Enter the network configuration file ifcfg-ethxy in the version checking tool:

```
# rcstool init /etc/sysconfig/network-scripts/ifcfg-eth<xy>
```

4. Reconfigure udev and reboot

   As root, on the VM, follow the steps below:

```
# udevadm control --reload
# udevadm trigger
# reboot
```

5. Pre-install consideration

   Before starting the Mediation software installation, if the PDU Record storage is deployed on the Management server (the "Troubleshooting" use case), use, in the bulkconfig file, for the PDU storage, the IP address of the Management server on the Storage network; if the PDU storage is an external server, put, in the bulkconfig file, the IP address of that external server.

   On the PDU storage server, is it the Management server or an external server, in the /etc/hosts file, be sure to put the IP address of the Mediation servers on the Storage network, otherwise the Mediation servers won't be allowed to connect to the PDU shared directory.

6. Post-install update of /etc/hosts

   After the Mediation software has been installed (after the "Integrate Customer Network" step), on each Mediation server, in the file /etc/hosts, put the IP addresses on the Prod3 network for the other Mediation servers.

   a. As root, check the /etc/hosts file out:

```
# rcstool co /etc/hosts
```

   b. Change the IP addresses of the other Mediation servers in /etc/hosts (use vi to update the file)

   c. Check the /etc/hosts file in:

```
# rcstool ci /etc/hosts
```

   Example of /etc/hosts file for the Mediation server 1c:

```
# cat /etc/hosts
127.0.0.1       localhost localhost4 localhost4.localdomain4
::1             localhost localhost6 localhost6.localdomain6
10.31.1.160     ntpserver1
10.31.2.56      nsp_oracle nsp_primary nsp_secondary (Backend network)
192.168.123.3 ixp1200-1a 1a             (Internal Production network Prod3)
192.168.123.4 ixp1200-1b 1b             (Internal Production network Prod3)
10.31.2.57      ixp1200-1c 1c                                   (Backend network)
```

Step 9 : Dataflows configuration

This step must be done through Management Application.

Any IP traffic manageable by the Performance Intelligence Center System, can be processed. Here is the example of the DSR Integrated Monitoring solution.

1. Configure the 12 Dataflows Load Balancing on Acquisition side.

   Be sure to modify the PDU filter DIA_LS_MAX depend of max load sharing destinations that you need and add to filters DIA_PORTS ports values, depending on customer site.

2. Create the 6 Dataflows per Mediation,

   Call them "Dia_<X><Y>", where <X> is the Mediation server number (1 for the first Mediation server and 2 for the second) and <Y> is the DFP number (from 1 to 6); select the builder "LTE Diameter TDR Reconstitution" with its default parameters and the following tuning:

   a. in IP Transport for item "Builders Subscriptions" of IMS Diameter, add the potential specific port values, depending of customer site

b. in IP Transport for “List of servers ports known” of Diameter, add the potential specific port values, depending of customer site

c. in IMS Diameter Decoding, select the “Activate Optimized Diameter Mode” to processs all type of Diameter interfaces.

Note: for each Mediation server, the 6 dataflows will use the production network declared in the Centralized Configuration (this is Prod1), but for the second Mediation server, they should use the production network Prod2; this can only be changed with SQL commands to run on the MGMT database. Use sqlplus command line:

```
> update cfg_ixp_stream set ip_address1='<Prod2IP>' where datasource_id in (select datasource_id from cfg_datasource where name like 'Dia_2%');
> commit;
```

where **<*Prod2IP*>** is the IP address of the Acquisition server in the Production network Prod2.

Step 10: Storage Configuration

This step must be done through Management Application. Here is the example of the DSR Integrated Monitoring solution.

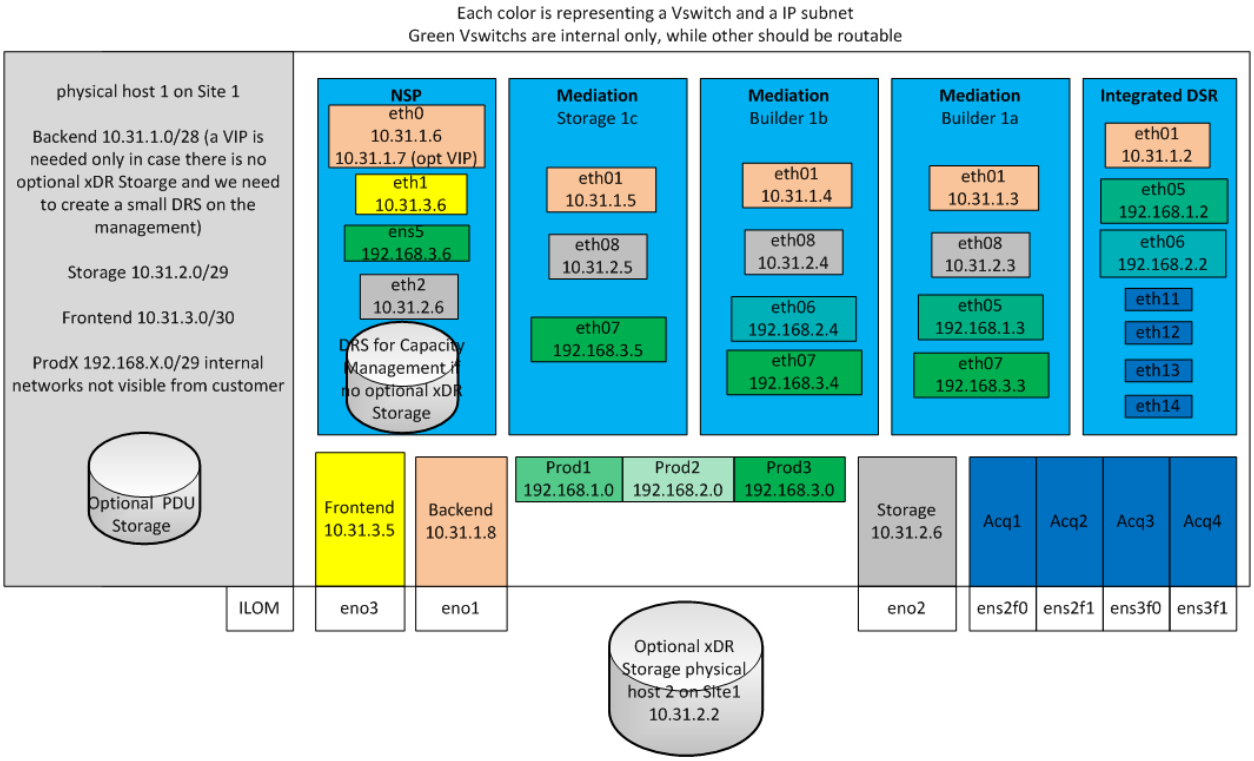
1. Use Case “Accounting”
   a. Activate the CSV option on Management Server
   b. Create the 12 Storages DFP by selecting the “Storage Type” = CSV Files
2. Use Case “Troubleshooting”

   Create the 12 Storages DFP by selecting the “Storage Type” = Datawarehouse

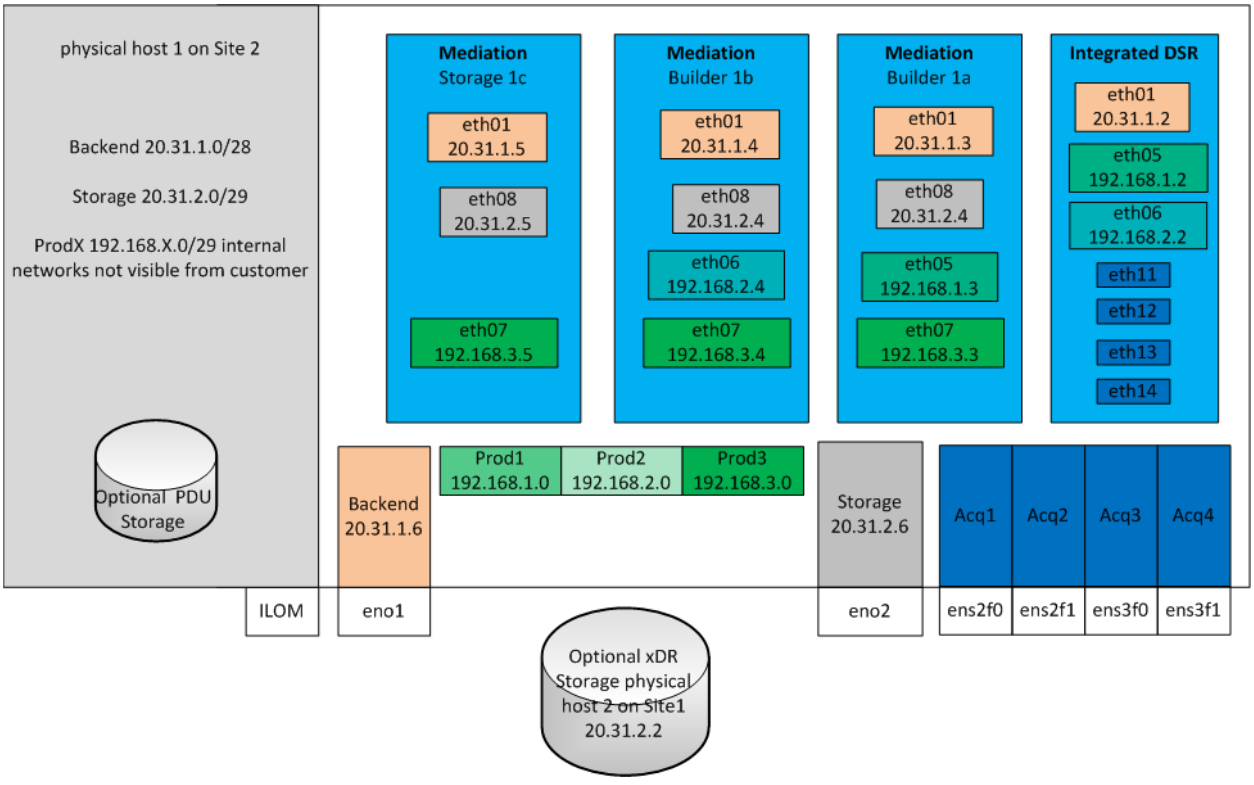
Detailed Schema

Here is a detailed representation of the prepackaged DSR Monitoring.

Site 1


Each color is representing a Vswitch and a IP subnet
Green Vswitchs are internal only, while other should be routable
physical host 1 on Site 1
Backend 10.31.1.0/28 (a VIP is needed only in case there is no optional xDR Stoarge and we need to create a small DRS on the management)
Storage 10.31.2.0/29
Frontend 10.31.3.0/30
ProdX 192.168.X.0/29 internal networks not visible from customer
Optional PDU Storage
NSP
eth0 10.31.1.6 10.31.1.7 (opt VIP)
eth1 10.31.3.6
ens5 192.168.3.6
eth2 10.31.2.6
DRS for Capacity Management if no optional xDR Storage
Mediation Storage 1c
eth01 10.31.1.5
eth08 10.31.2.5
eth07 192.168.3.5
Mediation Builder 1b
eth01 10.31.1.4
eth08 10.31.2.4
eth06 192.168.2.4
eth07 192.168.3.4
Mediation Builder 1a
eth01 10.31.1.3
eth08 10.31.2.3
eth05 192.168.1.3
eth07 192.168.3.3
Integrated DSR
eth01 10.31.1.2
eth05 192.168.1.2
eth06 192.168.2.2
eth11
eth12
eth13
eth14
Frontend 10.31.3.5
Backend 10.31.1.8
Prod1 192.168.1.0
Prod2 192.168.2.0
Prod3 192.168.3.0
Storage 10.31.2.6
Acq1
Acq2
Acq3
Acq4
ILOM
eno3
eno1
eno2
ens2f0
ens2f1
ens3f0
ens3f1
Optional xDR Storage physical host 2 on Site1 10.31.2.2

Site 2


physical host 1 on Site 2
Backend 20.31.1.0/28
Storage 20.31.2.0/29
ProdX 192.168.X.0/29 internal networks not visible from customer
Optional PDU Storage
Mediation Storage 1c
eth01 20.31.1.5
eth08 20.31.2.5
eth07 192.168.3.5
Mediation Builder 1b
eth01 20.31.1.4
eth08 20.31.2.4
eth06 192.168.2.4
eth07 192.168.3.4
Mediation Builder 1a
eth01 20.31.1.3
eth08 20.31.2.4
eth05 192.168.1.3
eth07 192.168.3.3
Integrated DSR
eth01 20.31.1.2
eth05 192.168.1.2
eth06 192.168.2.2
eth11
eth12
eth13
eth14
Backend 20.31.1.6
Prod1 192.168.1.0
Prod2 192.168.2.0
Prod3 192.168.3.0
Storage 20.31.2.6
Acq1
Acq2
Acq3
Acq4
ILOM
eno1
eno2
ens2f0
ens2f1
ens3f0
ens3f1
Optional xDR Storage physical host 2 on Site1 20.31.2.2

14. VIRTUAL INSTALLATION ON SUN X7-2

Configuration Overview

This configuration is targeted for customers who want to use PIC on virtual platform on hardware as specified in our Hardware Installation Guidelines document. The chapter is explained using SUN X7-2 server as hardware, however the procedures can be applied on other hardware types e.g. HP Gen 9, SUN X6-2

PIC 10.4.0 release is also virtualizing integrated acquisition server using openVswitch.

There is one to one mapping between guest and host, all the host hardware resources are reserved for the guest VM.

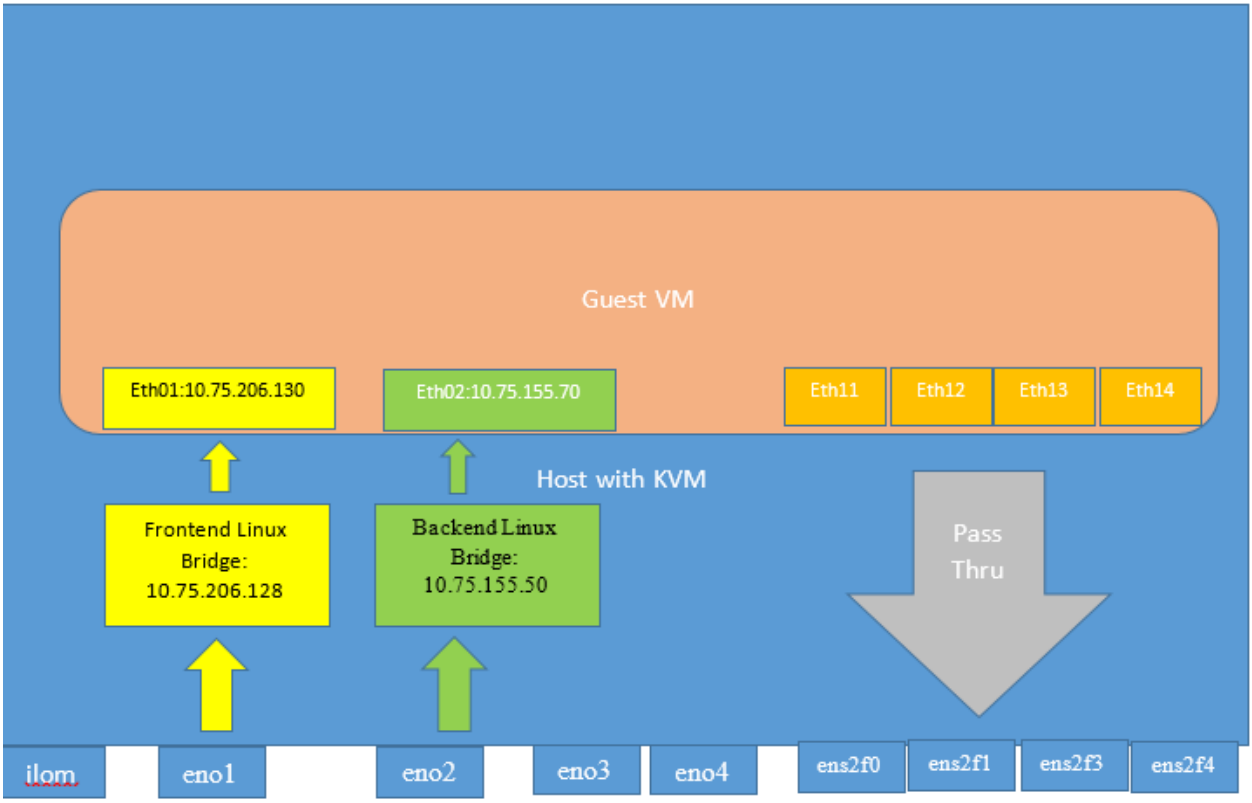


Figure 5: Management Virtualization

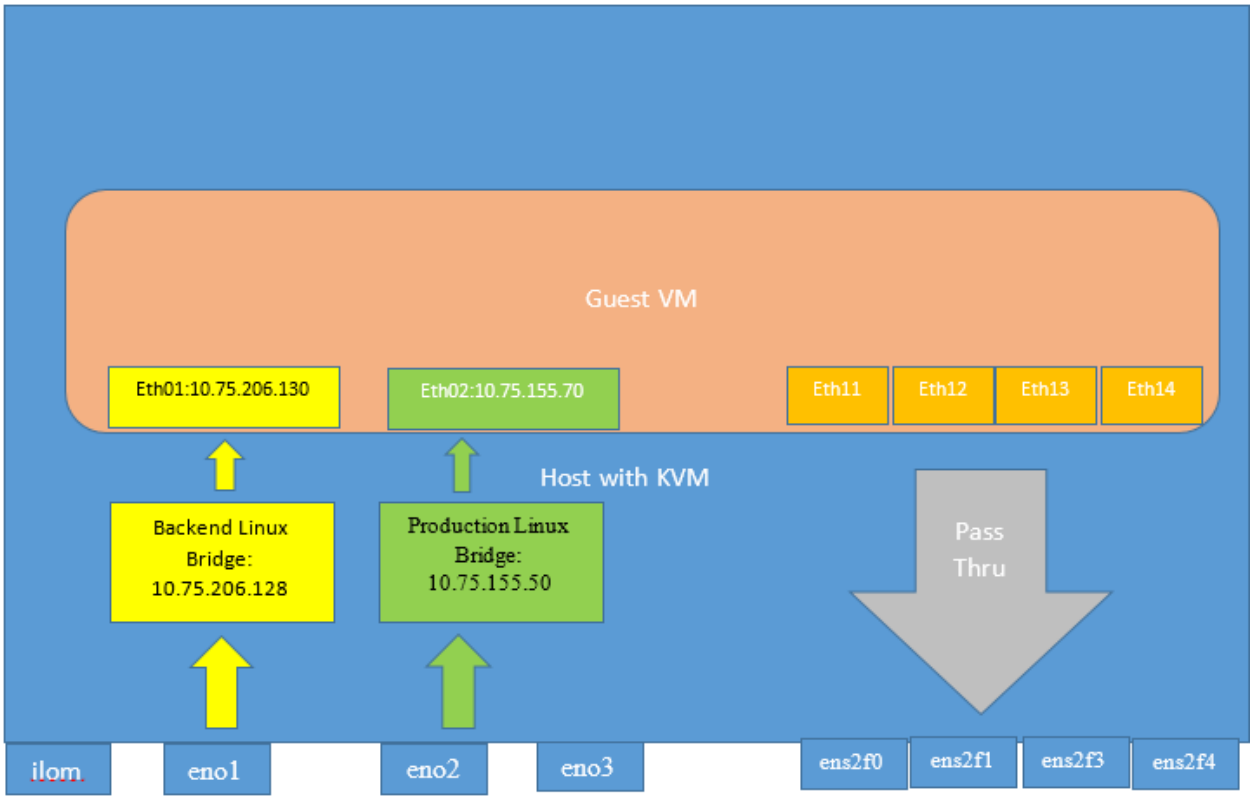


Figure 6: Probed and Mediation Virtualization

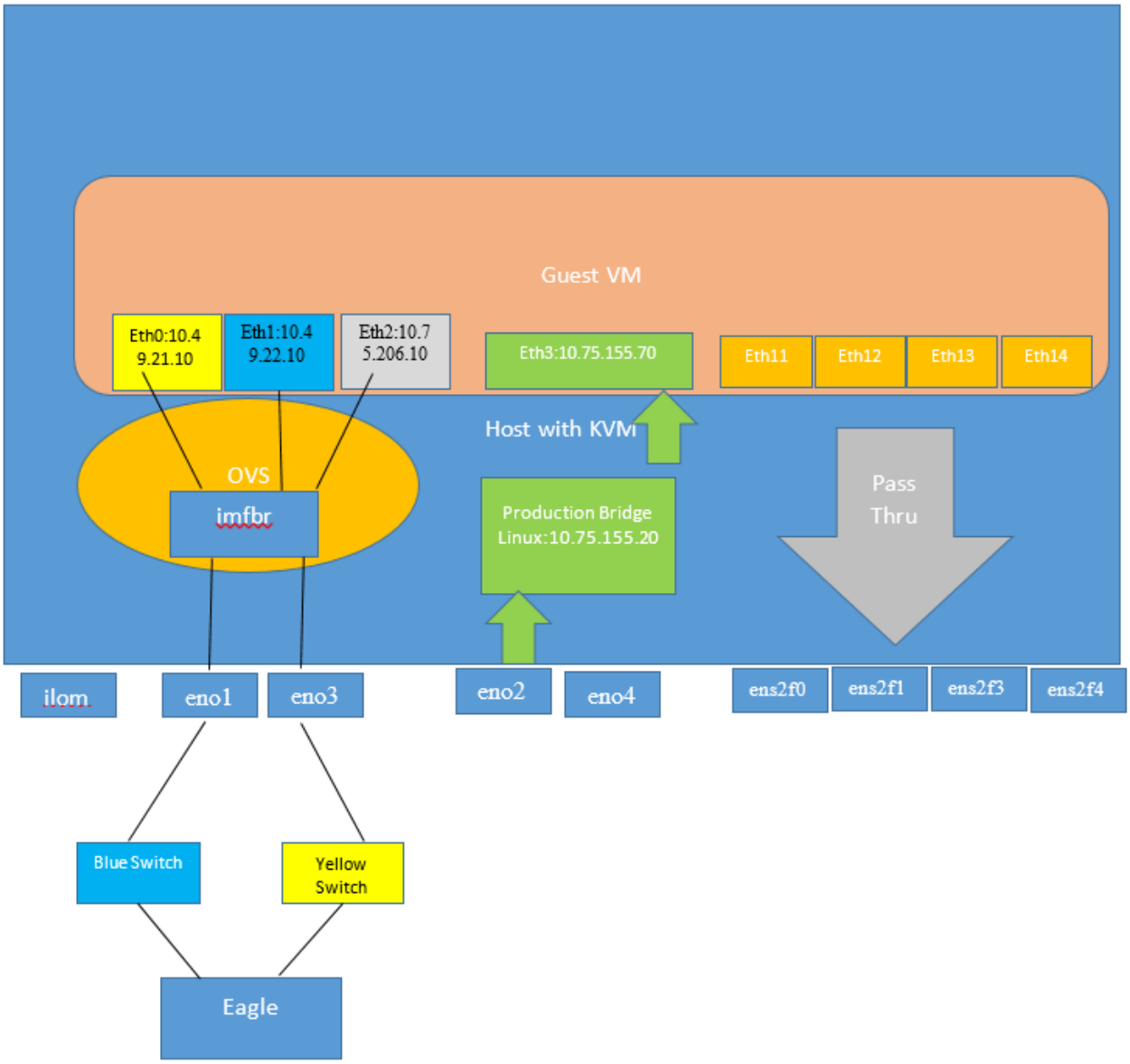


Figure 7: Integrated Acquisition Virtualization

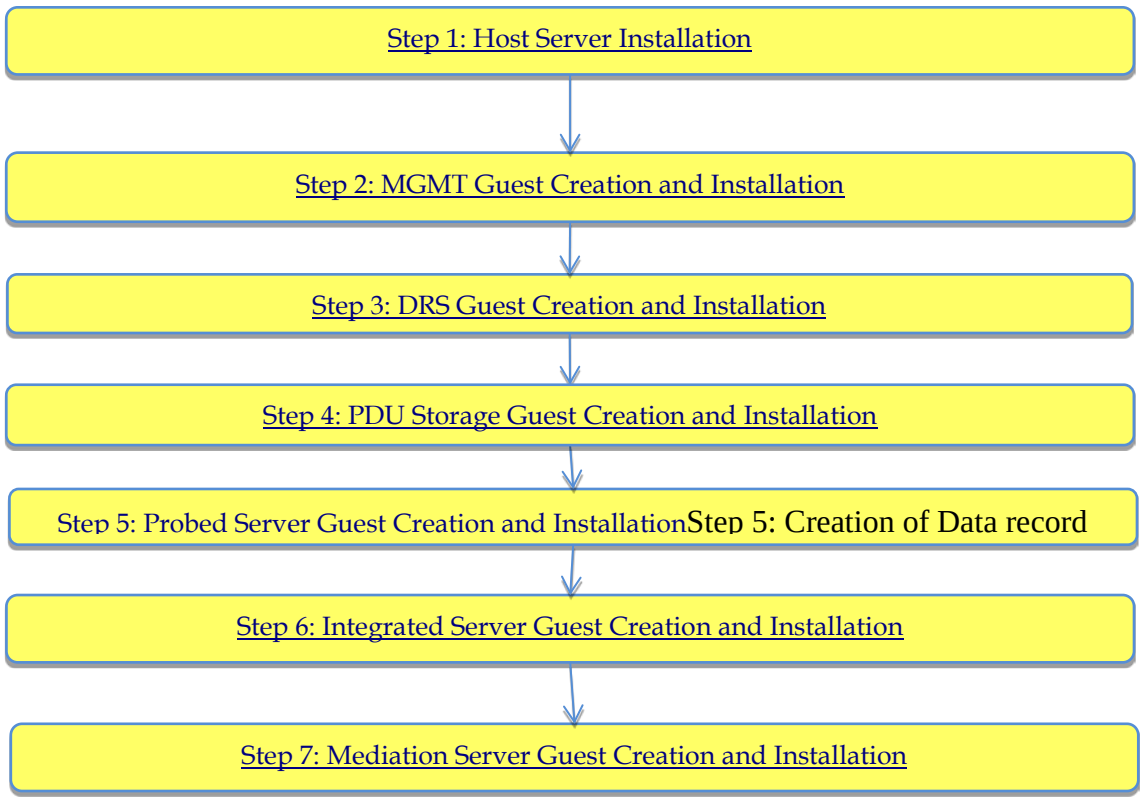
Configuration Steps

This chapter describes the steps to follow in a scrupulous manner to achieve the configuration of one guest per host.

Note1: KVM or VmWare can be used. Examples of commands are provided for KVM.

Note2: For Probed only the pass thru mode is enabled.

Note3: OVS will be used for integrated acquisition server configuration.



Step 1: Host Server Installation

This step must be done on all the available hosts.

(1) Installation of Oracle Linux
(2) NTP Configuration
(3) Enable PCI Pass through
The step 3 is only required when the IMF should be installed in Pass-through mode or when the capture cards should be pass through to the guest directly for PMF.
(4) Detach 10G Links
The step 4 is only required when the PMF should be installed, so that 10G cards are detached on the host and could be reattached to the guests.
(5) **Network configuration** help in the creation of
    a. Backend Bridge (Mandatory for all hosts): for the communication between different PIC components regarding configuration and processing.
    b. Frontend Bridge (optional): for Mgmt GUI web browser access.
    c. External Production Bridge (optional): for communication between mediation and acquisition server during processing of PDUs only. This is needed to separate the production and management network.
    d. Internal Production bridges for high performance between VM Acquisition & Mediation.

Configure the network bridges as indicated below:

a. Backend Bridge
    a. Create one Backend bridge using “nmtui” tool, if no GUI is available to create bridges.
    b. Add Ethernet interface in the bridge.
    c. Provide the IP address and route to the bridge. Add default route on this bridge.
b. Frontend Bridge (only for the MGMT host)
    a. Create one Frontend bridge using “nmtui” tool, if no GUI is available to create bridges.
    b. Add Ethernet interface in the bridge.
    c. Provide the IP address (from different subnet than Backend bridge) and route to the bridge. Add default route on this bridge.
c. External Production bridge, named **ExtProd**
    a. Proceed as for the Backend bridge but with DEFROUTE=no
d. Internal Production bridges for high performance between VM Acquisition & Mediation

    a. This bridge, named Prod1, allow **internal** server communication between the VMs. *Add no Bridged Connections*.

    b. Give a name to the bridge, e.g “**Prod1**”, give an IP Address and set DEFROUTE=no

(6) Open vSwitch (OVS) Configuration for **integrated acquisition host**

a. Installation of OVS on host

    i. Refer the OVS official Link OVS.org to download the OVS tar ball from its Download Section. Prefer to download the LTS version as it is stable to use.The one used for current installation is This.(openvswitch-2.5.4.tar.gz)
    ii. Refer the Installation procedure for OVS tar ball using this Installation_Proc.
    iii. Make sure to configure the ovs-ctl service so that it is started automatically on reboot.

b. Create a bond interface as bond0 and enslave the physical interfaces that are connected to the yellow and blue Cisco switches. Assuming two physical interfaces are eno1 and eno3
    i. Create following network configuration for eno1, vi /etc/sysconfig/network-scripts/ifcfg-eno1

    BOOTPROTO=none
    MTU=2000
    MASTER=bond0
    ONBOOT=yes
    TYPE=Ethernet
    DEVICE=eno1
    SLAVE=yes
    NM_CONTROLLED=NO

    ii. Create following network configuration for eno3, vi /etc/sysconfig/network-scripts/ifcfg-eno3

    BOOTPROTO=none

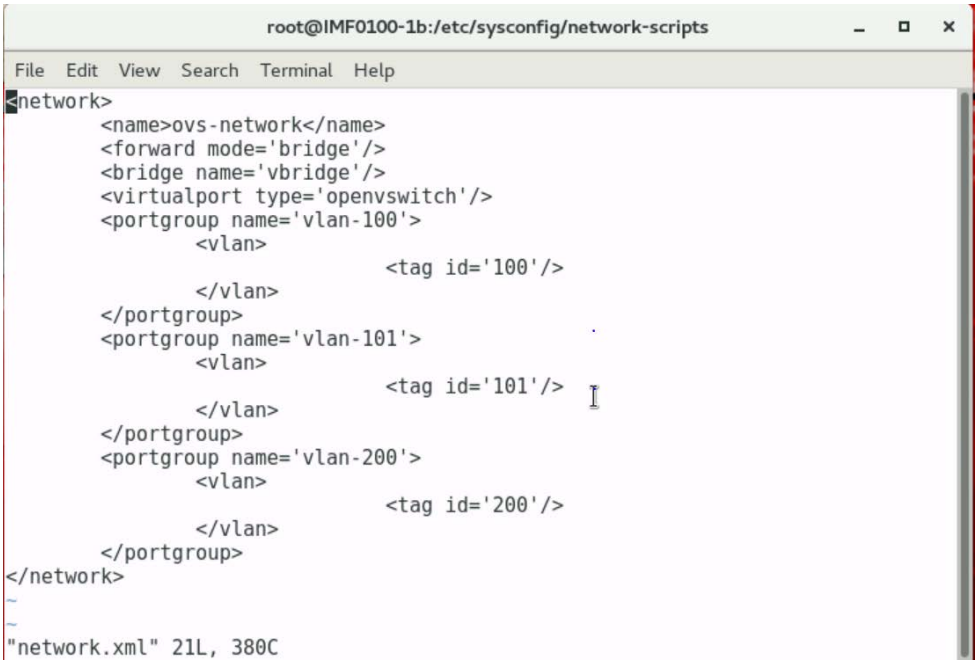
    MTU=2000
    MASTER=bond0
    ONBOOT=yes

TYPE=Ethernet
DEVICE=eno3
SLAVE=yes
NM_CONTROLLED=no

iii. Create the following configuration for the bond0, vi /etc/sysconfig/network-scripts/ifcfg-bond0

MTU=2000
BOOTPROTO=none
BONDING_OPTS="mode=active-backup miimon=100 primary=eno1 updelay=100 downdelay=100"
BOND_INTERFACES=eno1,eno3
ONBOOT=yes
TYPE=Bonding
DEVICE=bond0

c. Create the bridge using OVS and bond0 interface to the bridge
   i. ovs-vsctl add-br imfbr0 stp_enable=true
   ii. ovs-vsctl add-port imfbr0 bond0
d. Create one network in open vSwitch, use the following steps
   i. Create a network configuration file "network.xml" at /etc/sysconfig/network-scripts/
   ii. Add the following content in the networl.xml file, refer the attached screen shot
      - Name the network as "ovs-network"
      - Set the forward mode as bridge
      - Bridge name as imfbr0 (created in the previous step)
      - Virtualport type as "openvswitch"
      - Provide the port groups with VLAN tags, three portgroups need to be added for the Yellow VLAN (100), Blue VLAN (101) and Management VLAN(200)



iii. Execute the following commands to define and start the network created in previous step

- # virsh net-define /etc/sysconfig/network-scripts/network.xml
- # virsh net-destroy ovs-network
- # virsh net-start ovs-network
- # ovs-ctl stop
- # ovs-ctl start

Note: In case the network definition needs to be changed then, all the above mentioned commands need to be executed again. In case the VMs are using the ovs network created above, the VMs should be shutdown and start again.

iv. Make the OVS network created in previous step as auto-start in case of reboot

The below command will mark the ovs-network for auto-start

virsh net-autostart ovs-network

The below command will list all the networks that are defined in OVS

virsh net-list --all

```
[root@IMF0100-1b ~]# virsh net-list --all
 Name                 State      Autostart     Persistent
----------------------------------------------------------
 default              active     yes           yes
 ovs-network          active     yes           yes
```

Note: The above created ovs-network will be used during the creation of IMF guest

Step 2: MGMT Guest Creation and Installation

Management Server must be installed only one time for the Performance Intelligence Center system to manage. Refer to Chapter 9 for OL based Installation.

Note: The guest creation is explained using virsh command line utility, however user can also create VMs using the virtual machine manager utility, which is a GUI based tool.

Management Guest Creation

1. Create VM

```
# virt-install --virt-type kvm --hvm --connect qemu:///system --network bridge=Backend,model=virtio --network bridge=Frontend,model=virtio --cdrom /var/ORCL/V74844-01.iso --disk path=/var/vm_server/MGMT.disk,size=800,sparse=no,bus=ide --name MGMT --autostart --boot cdrom,hd --ram 266240 --vcpus 92 --graphics vnc --os-variant rhel6
```

2. The following arguments are to be provided to the virt-install command:
    - Virtualization mode: --virt-type kvm --hvm --connect qemu:///system
    - Network interfaces (keep the order):
        - Management: --network bridge=<*backend*>,model=virtio
        - GUI Access: --network bridge=<*Frontend*>,model=virtio
    - Boot order: --boot cdrom,hd
    - CD drive: --cdrom <*OL ISO File*>
    - Disk: --disk path=<*disk_file*>,size=<*disk_size*>,sparse=no,bus=ide
    - VM name: --name <*vm_name*>

- RAM: --memory <*ram_size*>
- CPU: --vcpus <*cpu_count*>,cpuset=<*cpu_set*>
- Display: --graphics vnc
- VM optimization: --os-variant rhel6

where

- <*backend*> is the name of the network bridge used for the management network, in this case it is **Backend**.
- <*frontend*> is the name of the network bridge used for the web browser access, in this case it is **Frontend**.
- <*OL ISO File*> is the full path and name of the OL ISO file
- <*disk_file*> is the full path and name of the disk file (be sure to create it on a file system having enough space)
- <*disk_size*> is the size (in GB) of the disk to create
- <*vm_name*> is the name of the VM (preferably use letters, digits, underscores and hyphens)
- <*ram_size*> is the size (in GB) of RAM to allocate to the VM; do not over allocate as the host itself and all of the guests will use RAM
- <*cpu_count*> is the number of CPU to allocate to the VM; do not over allocate as the host itself and all of the guests will use CPU

Add external disks to the MGMT VM

After the MGMT VM has been created and Oracle Linux has been installed on the virtual machine as a result of the previous step "Management Guest Creation", the additional external disks should be made available to the VM. These disks will be used to create the ASM disk group for Oracle database installation. Perform the following steps

1. Edit the MGMT virtual machine property file. For this machine has to be in shutdown state.
   a. Enter virsh command prompt, execute

```
# virsh
```

   b. Edit the MGMT VM property file, execute

```
virsh #    shutdown MGMT
virsh #    edit MGMT
It will open the property file in vi editor mode, look for <devices> tag. In the devices section add additional external disks entries. The entries will look like as mentioned below
<disk type='block' device='disk'>
        <driver name='qemu' type='raw'/>
        <source dev='/dev/sdc'/>
        <target dev='hdc' bus='scsi'/>
        <address type='drive' controller='0' bus='0' target='0' unit='2'/>
</disk>
Here /dev/sdc is the external device name, target device name could be anything of your choice, preference "hdc". Choose carefully unit='2', this denotes the numbering of the devices in the VM, unit='0' or unit='1' might have already been assigned to the system disk and cdrom drive.

After additions have made to the property file, save the file as in vi editor.

# Start the VM
Virsh # start MGMT
```

2. Proceed with ASM disk configuration.

Note: Care should be taken as in guests the master disk (system disk) or additional disk names can be swapped e.g. “hdb” can be system disk and “hda” can be additional disk. Please ensure that for ASM creation only the additional disks are used and system disks are not touched.

Install Oracle ASM

Refer Installation of Oracle ASM

Install Management Server

Refer Installation of Management Server

Management Server Guest OS Reinstallation

Refer steps from Management Guest OS reinstallation

Step 3: DRS Guest Creation and Installation

DRS Guest creation and installation involves creation of DRS VM, addition of external disks, ASM installation on the external disks and schema creation. Refer to Chapter 9 for OL based Installation.

DRS Guest Creation

Note: The guest creation is explained using virsh command line utility, however user can also create VMs using the virtual machine manager utility, which is a GUI based tool.

1. Create VM

```
# virt-install --virt-type kvm --hvm --connect qemu:///system --network bridge=Backend,model=virtio --cdrom /var/ORCL/V74844-01.iso --disk path=/var/vm_server/DRS.disk,size=800,sparse=no,bus=ide --name DRS --autostart --boot cdrom,hd --ram 266240 --vcpus 90 --graphics vnc --os-variant rhel6
```

2. The following arguments are to be provided to the virt-install command:
    - Virtualization mode: --virt-type kvm --hvm --connect qemu:///system
    - Network interfaces (keep the order):
        - Management: --network bridge=<*Backend*>,model=virtio
    - Boot order: --boot cdrom,hd
    - CD drive: --cdrom <*OL ISO File*>
    - Disk: --disk path=<*disk_file*>,size=<*disk_size*>,sparse=no,bus=ide
    - VM name: --name <*vm_name*>
    - RAM: --memory <*ram_size*>
    - CPU: --vcpus <*cpu_count*>,cpuset=<*cpu_set*>
    - Display: --graphics vnc
    - VM optimization: --os-variant rhel6

    where
    - <*backend*> is the name of the network bridge used for the management network, in this case it is **Backend**.
    - <*OL ISO File*> is the full path and name of the OL ISO file
    - <*disk_file*> is the full path and name of the disk file (be sure to create it on a file system having enough space)

- <*disk_size*> is the size (in GB) of the disk to create
- <*vm_name*> is the name of the VM (preferably use letters, digits, underscores and hyphens)
- <*ram_size*> is the size (in GB) of RAM to allocate to the VM; do not over allocate as the host itself and all of the guests will use RAM
- <*cpu_count*> is the number of CPU to allocate to the VM; do not over allocate as the host itself and all of the guests will use CPU

Addition of external disks in DRS Guest

Refer Addition of external disks to VM, in this customize the steps for DRS e.g. replace the name of DRS VM while editing the virtual machine property file.

ASM Installation on DRS Guest

This step must be done on the server hosting DRS.

Refer to the document Oracle ASM and database on Third-Party Server Installation

Create database and schema on DRS Guest

Refer Data WareHouse Server (DWS) for DWS schema Installation.

OS Reinstallation on DRS Guest

In order to reinstall the OS, the ISO file of the Oracle linux is needed on the host

Use this procedure when the OS is to be reinstalled on an existing guest (the previous section explains how to create a new guest):

1. Open an X terminal as root
2. Reinstall the OS on the existing guess:
   - open the guest’s console: virt-viewer <*vm_name*> &
   - find the target name of the CDROM device (get the value in the Target column, on the cdrom line): virsh domblklist <*vm_name*> --details
   - attach the OS disk: virsh attach-disk <*vm_name*> <*tpd_iso_file*> <*target*> --type cdrom --mode readonly
   - reboot the guest: virsh reboot <*vm_name*>. **Don’t forget to check the reboot order.**

   Where,
   - <*vm_name*> is the name of the VM
   - <*tpd_iso_file*> is the full path and name of the TPD ISO file
   - <*target*> is the target name of the CDROM device on the VM

   Example:

```
# virt-viewer DRS &
# virsh domblklist DRS --details
Type         Device       Target       Source
-----------------------------------------------
```

```
file        disk        hda         /var/vm_server/DRS.disk
block       cdrom       hdb         -
file        disk        hdc         /var/lib/libvirt/images/DRS.qcow2
block       disk        hdd         /dev/sdb1
# virsh attach-disk /var/ORCL/V74844-01.iso hdb --type cdrom --mode readonly
# virsh reboot DRS
```

Note: after the server has rebooted, it might be possible that the Oracle linux ISO has not been ejected. In this case, the ISO has to be manually ejected and the server restarted. Example:

```
# virsh destroy DRS
# virsh change-media DRS hdb --eject
# virsh start DRS
```

3. Installation of Oracle Linux
   Refer to the chapter Oracle linux on Third-Party Server Installation

   a. Hostname configuration
      Configure in /etc/hosts file the IP address which contain the backend IP address
   b. Default Linux installation tuning
      System Partitioning Recommendation

Step 4: PDU Storage Guest Creation and Installation

PDU storage guest creation and installation involves creation of guest VM, addition of external disks, OL installation. Refer to Chapter 9 for OL based Installation.

PDU Storage Server Guest Creation

Note: The guest creation is explained using virsh command line utility, however user can also create VMs using the virtual machine manager utility, which is a GUI based tool.

1. Create VM

```
# virt-install --virt-type kvm --hvm --connect qemu:///system --network bridge=Backend,model=virtio --cdrom
/var/ORCL/V74844-01.iso --disk path=/var/vm_server/PDU.disk,size=800,sparse=no,bus=ide --name PDU --
autostart --boot cdrom,hd --ram 266240 --vcpus 90 --graphics vnc --os-variant rhel6
```

2. The following arguments are to be provided to the virt-install command:
   - Virtualization mode: --virt-type kvm --hvm --connect qemu:///system
   - Network interfaces (keep the order):
     - Management: --network bridge=<*Backend*>,model=virtio
   - Boot order: --boot cdrom,hd
   - CD drive: --cdrom <*OL ISO FILE*>
   - Disk: --disk path=<*disk_file*>,size=<*disk_size*>,sparse=no,bus=ide
   - VM name: --name <*vm_name*>
   - RAM: --memory <*ram_size*>
   - CPU: --vcpus <*cpu_count*>,cpuset=<*cpu_set*>
   - Display: --graphics vnc
   - VM optimization: --os-variant rhel6

   Where,

- <*backend*> is the name of the network bridge used for the management network, in this case it is **Backend**.
- <*OL ISO File*> is the full path and name of the OL ISO file
- <*disk_file*> is the full path and name of the disk file (be sure to create it on a file system having enough space)
- <*disk_size*> is the size (in GB) of the disk to create
- <*vm_name*> is the name of the VM (preferably use letters, digits, underscores and hyphens)
- <*ram_size*> is the size (in GB) of RAM to allocate to the VM; do not over allocate as the host itself and all of the guests will use RAM
- <*cpu_count*> is the number of CPU to allocate to the VM; do not over allocate as the host itself and all of the guests will use CPU

Addition of external disks in PDU Storage Guest

Refer Addition of external disks to VM, in this customize the steps for PDU server e.g. replace the name of PDU server VM while editing the virtual machine property file.

PDU Storage(s) Installation

Refer Packet Data Unit Storage (PDU) Installation.

PDU Storage Server Guest OS Reinstallation

Refer steps similar to the procedure Guest OS Re-Install, customize the steps for PDU storage server.

Step 5: Probed Server Guest Creation and Installation

The procedures in this section shall involve the probed server guest creation, where the host capturing devices will pass through the guest. The section will also describe the procedure of OS re-installation on the guest.

Probed Server Guest Creation

Note: The guest creation is explained using virsh command line utility, however user can also create VMs using the virtual machine manager utility, which is a GUI based tool.

Refer steps from section “Probed Guest Creation”. Use only Backend bridge, however if the external production bridge is needed then adapt the command accordingly. Customize the hardware resources as needed on SUN X7-2.

After the guest is created and application is installed, integrate the server with CCM application using steps explained in chapter Configure Site and Subsystem for Acquisition Server. Make sure the JRE is already installed before discovering the acquisition sub-system on CCM.

Probed Server Guest OS Reinstallation

Refer steps from the section Probed Guest OS reinstallation

Probed Server network device configuration

Refer steps from the section Probed Guest network devices configuration

Step 6: Integrated Server Guest Creation and Installation

Integrated Server Installation using Open vSwitch

The procedures in this section shall involve the integrated acquisition server guest creation. This host should have the Open vSwitch already installed on it and one bridge using Open vSwitch (OVS) should already be created. The Open vSwitch installation has already been done as part of **Host server installation** in **Step1, sub-step 6**.

The section will also describe the procedure of OS re-installation on the guest.

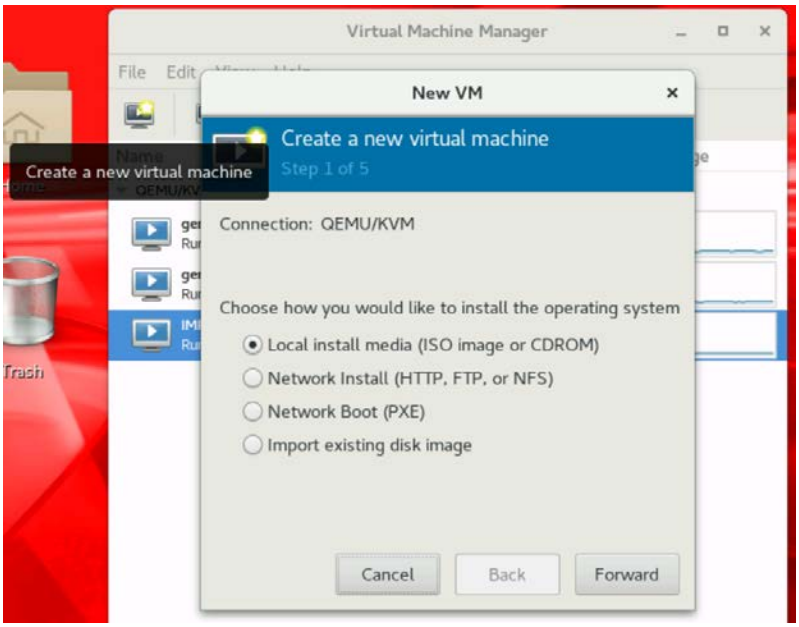
Integrated Acquisition Server Guest Creation

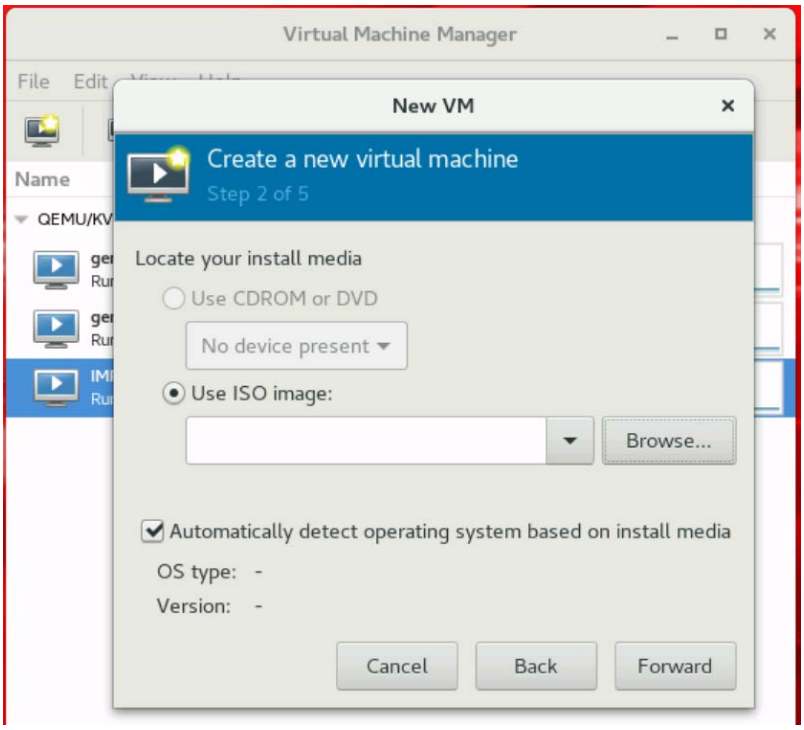
Note: The guest creation is explained using the virtual machine manager utility, which is a GUI based tool.

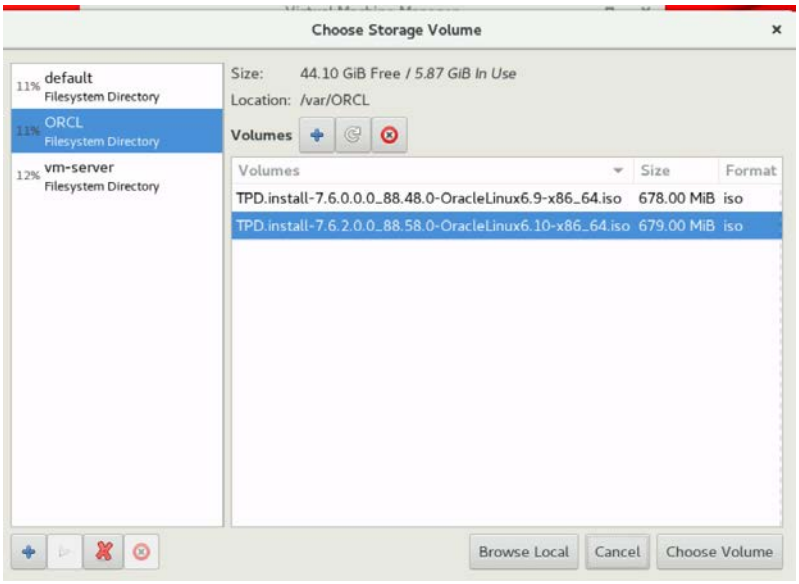
These steps should be performed for all the guests that needs to be created.

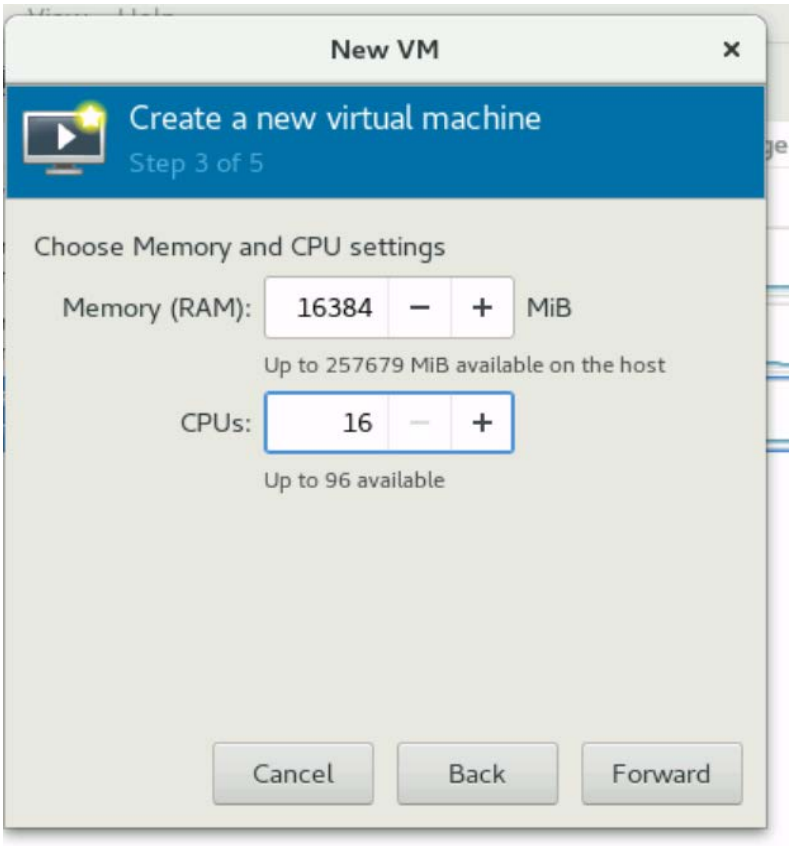
1. Create a VM
    - Login to the ILO of HOST machine using its graphical interface.
    - Go to System Tools -> VMM

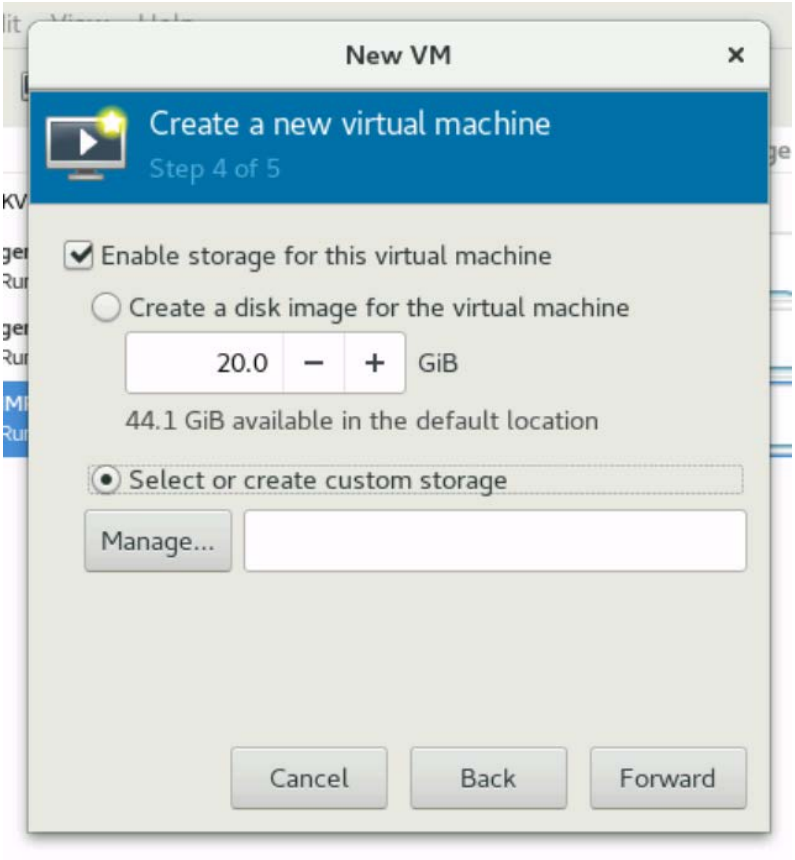
    - Launch a VM using 62 GB of RAM, 22 vCPU, 200 GB of volume storage

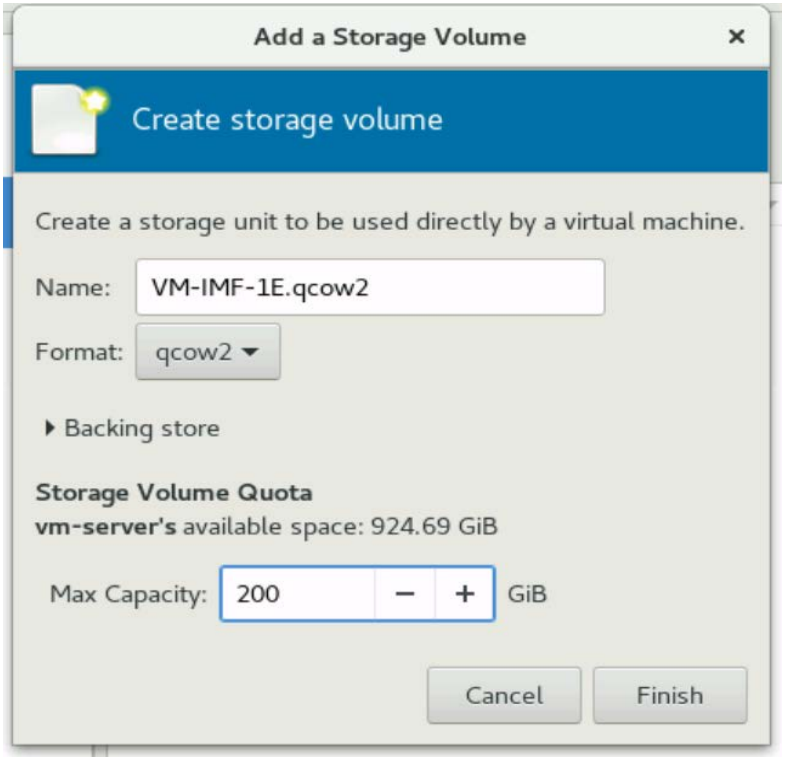


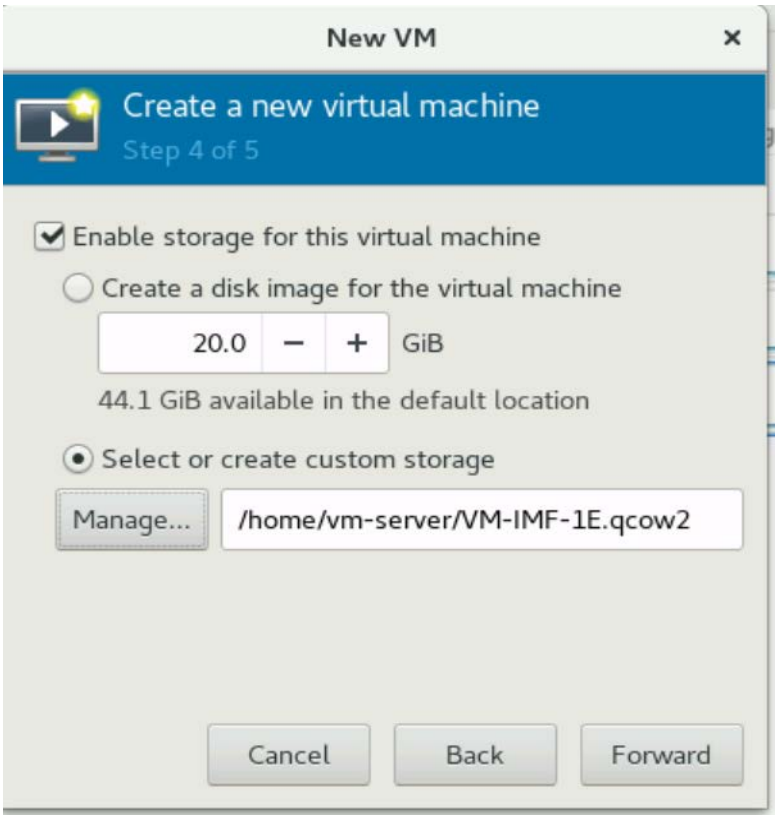

Virtual Machine Manager
File Edit
Name
QEMU/KV
New VM
Create a new virtual machine
Step 2 of 5
Locate your install media
Use CDROM or DVD
No device present
Use ISO image:
Browse...
Automatically detect operating system based on install media
OS type: -
Version: -
Cancel
Back
Forward

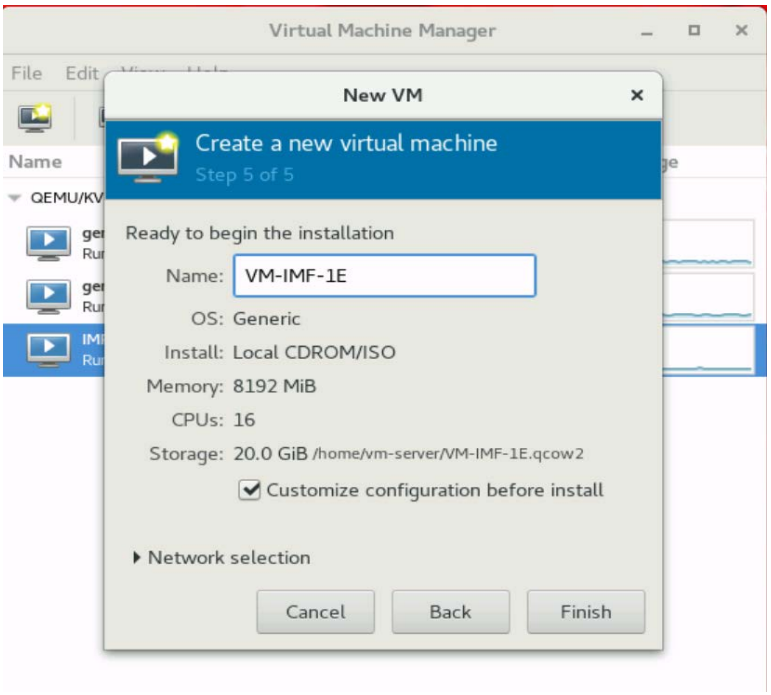

Choose Storage Volume
default
Filesystem Directory
ORCL
Filesystem Directory
vm-server
Filesystem Directory
Size: 44.10 GiB Free / 5.87 GiB In Use
Location: /var/ORCL
Volumes
Volumes
Size
Format
TPD.install-7.6.0.0.0_88.48.0-OracleLinux6.9-x86_64.iso 678.00 MiB iso
TPD.install-7.6.2.0.0_88.58.0-OracleLinux6.10-x86_64.iso 679.00 MiB iso
Browse Local
Cancel
Choose Volume


New VM
Create a new virtual machine
Step 3 of 5
Choose Memory and CPU settings
Memory (RAM):
16384
MiB
Up to 257679 MiB available on the host
CPUs:
16
Up to 96 available
Cancel
Back
Forward


New VM
Create a new virtual machine
Step 4 of 5
Enable storage for this virtual machine
Create a disk image for the virtual machine
20.0
GiB
44.1 GiB available in the default location
Select or create custom storage
Manage...
Cancel
Back
Forward

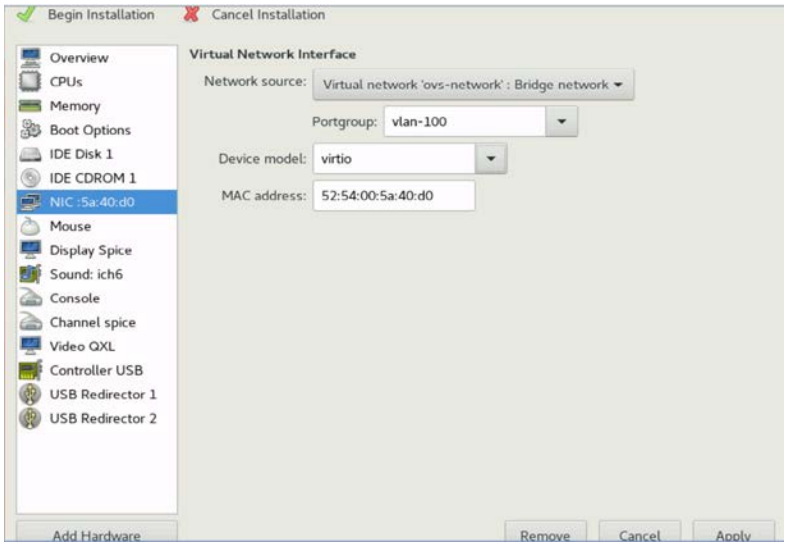

Add a Storage Volume
Create storage volume
Create a storage unit to be used directly by a virtual machine.
Name:
VM-IMF-1E.qcow2
Format:
qcow2
Backing store
Storage Volume Quota
vm-server's available space: 924.69 GiB
Max Capacity:
200
GiB
Cancel
Finish

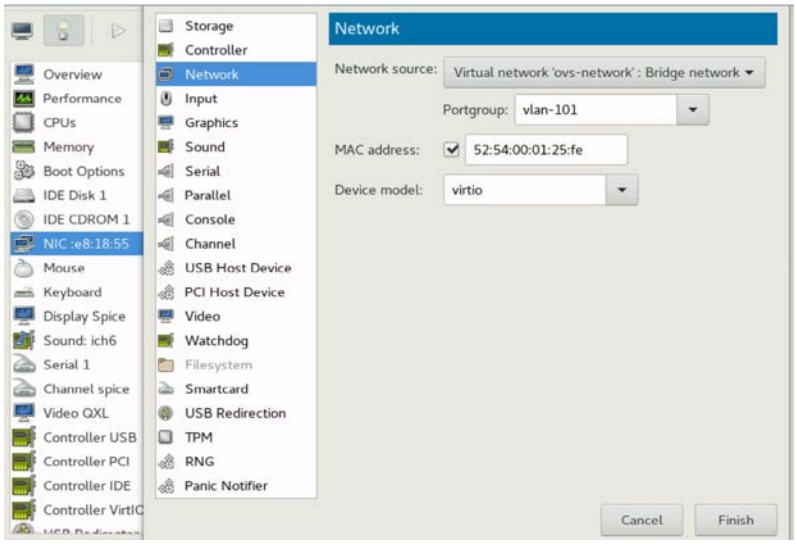


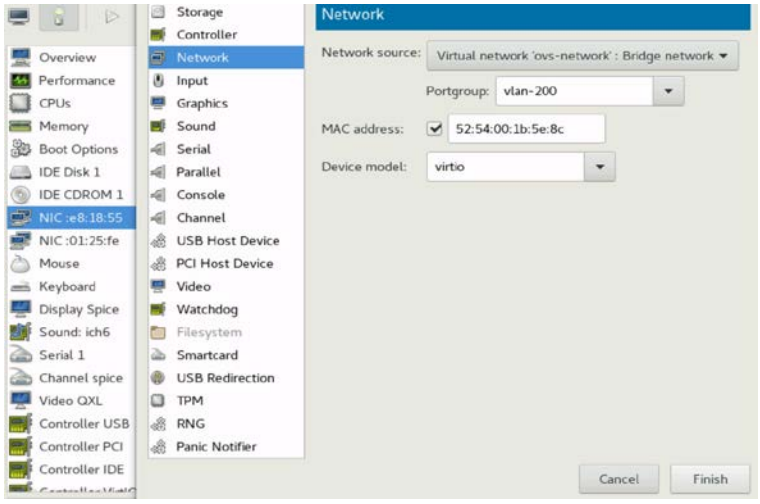


- Add and configure the network interfaces for the guest, 3 interfaces needs to be added. One NIC interface will be assigned Portgroup vlan-100 for Yellow VLAN, second NIC interface will be

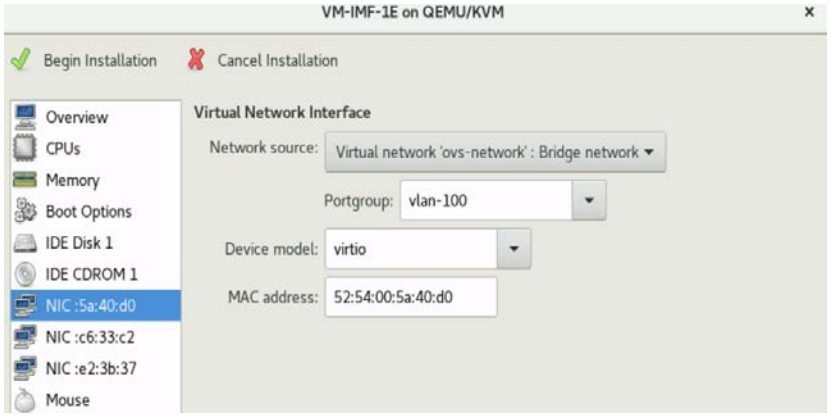
assigned Portgroup vlan-101 for Blue VLAN and third NIC interface will be assigned Portgroup vlan-200 for Management VLAN. Refer the below screen shots



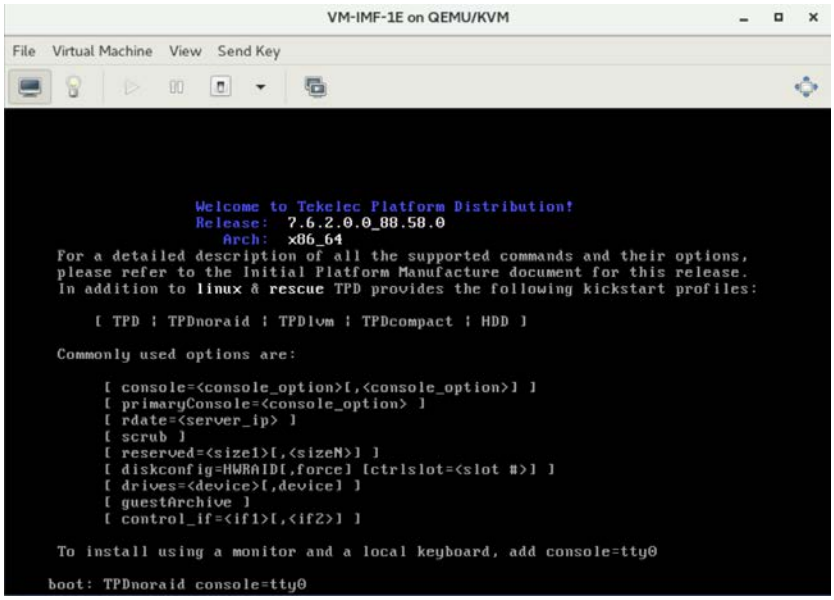




- Begin the OS installation on the machine by clicking Begin Installation. Refer below screen shot



Following TPD prompt will appear, enter TPDnoraid console=tty0



Verify Network devices configuration for integrated acquisition server guest

Verify if the guest’s vnet interfaces are attached to the ovsbridge.

```
# ovs-vsctl list-br
# ovs-vsctl list-ports <bridge name>
# ovs-ofctl show <bridge name>
```

```
[root@IMF09071B ~]# ovs-vsctl show
720b0725-22dd-40d8-9283-b34e36a2a1f6
    Bridge "imfbr0"
        Port "vnet1"
            tag: 101
            Interface "vnet1"
                type: internal
        Port "eno3"
            Interface "eno3"
        Port "vnet2"
            tag: 200
            Interface "vnet2"
                type: internal
        Port "eno1"
            Interface "eno1"
        Port "imfbr0"
            Interface "imfbr0"
                type: internal
        Port "vnet0"
            tag: 100
            Interface "vnet0"
                type: internal
    ovs_version: "2.5.4"
```

2. Proceed with Integrated acquisition server application installation.

Integrated Acquisition Server application installation on guest

Note: Care must be taken for the bulkconfig file for the virtual IMF. Refer Appendix B for more information on the Acquisition server bulkconfig file format.

1. Provide the temporary IP address to the eth2 interface of the guest and copy the application ISO.
2. Refer to the section Install Acquisition Server Application for installing application.
3. Refer to the section Configure Site and Subsystem for Acquisition Server for integration with CCM application and discovery of the sub-system on CCM.
4. After the IMF server installation is completed, verify the following on the IMF guest VMs
    - If **/etc/resolv.conf** file is present and it has nameserver entry e.g. nameserver 192.168.122.1. Then this entry should be commented out and **TKLCmf** service should be re-started.

OS Reinstallation on Integrated acquisition server guest

In order to reinstall the OS, the ISO file of the TPD is needed on the host.

Use this procedure when the OS is to be reinstalled on an existing guest (the previous section explains how to create a new guest):

1. Open an X terminal as root
2. Reinstall the OS on the existing guess:
   - open the guest’s console: virt-viewer <*vm_name*> &
   - find the target name of the CDROM device (get the value in the Target column, on the cdrom line): virsh domblklist <*vm_name*> --details
   - attach the OS disk: virsh attach-disk <*vm_name*> <*tpd_iso_file*> <*target*> --type cdrom --mode readonly
   - reboot the guest: virsh reboot <*vm_name*>. **Don’t forget to check the reboot order.**

   where
   - <*vm_name*> is the name of the VM
   - <*tpd_iso_file*> is the full path and name of the TPD ISO file
   - <*target*> is the target name of the CDROM device on the VM

   Example:

```
# virt-viewer VM_IMF_1A &
# virsh domblklist VM_IMF_1A --details
Type         Device       Target     Source
------------------------------------------------
file         disk         hda        /var/vm_server/VM_IMF_1A.disk
block        cdrom        hdb        -
file         disk         hdc        /var/lib/libvirt/images/VM_IMF_1A.qcow2
block        disk         hdd        /dev/sdb1
# virsh attach-disk /home/TPD.install-7.6.0.0.0_88.48.0-OracleLinux6.9-x86_64.iso hdb --type cdrom --mode
readonly
# virsh reboot VM_IMF_1A
```

   Note: after the server has rebooted, it might be possible that the TPD ISO has not been ejected. In this case, the ISO has to be manually ejected and the server restarted. Example:

```
# virsh destroy VM_IMF_1A
# virsh change-media VM_IMF_1A hdb --eject
# virsh start VM_IMF_1A
```

3. Installation of TPD

   Refer section, Table 1

Multiple VM guests on the single hosts

Refer the table below for the hardware resource sharing for multiple VMs on SUNX7-2 server

Function	vCPU	Minimum RAM	Minimum HDD	Configuration
Hypervisor	4	4	200 GB (*)	(*) This disk volume is what remains on the host

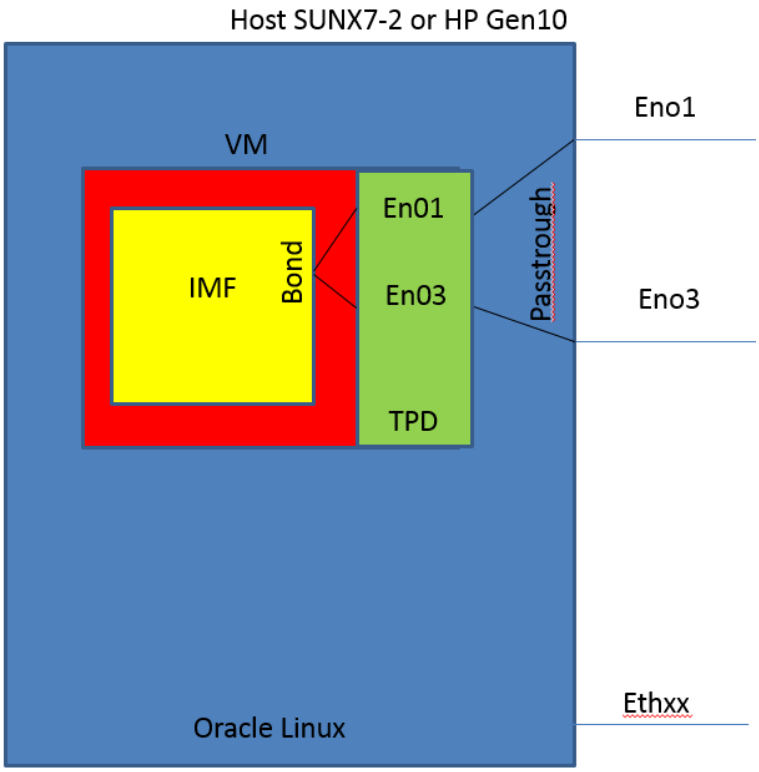
Int. Acq. VM 1 (imf1030-1a	22	62	200 GB	
Int. Acq. VM 2 (imf1030-1b	22	62	200 GB	
Int. Acq. VM 3 (imf1030-1c	22	62	200 GB	
Int. Acq. VM 4 (imf1030-1d	22	62	200 GB	

To create and install the guests VMs follow the procedures mentioned in Integrated Acquisition Server Guest Creation. Customize the hardware resources for the VM as indicated in table Table 6.

Table 5: Hardware resources for the multiple integrated acquisition server guests

Integrated Server Installation using Pass through

In case of pass through, the host’ s management interfaces e.g. eno1, eno2, eno3 and eno4 will be detached from the host and assigned to the guest directly.



(1) Installation of Oracle Linux
(2) NTP Configuration
(3) Enable PCI Pass through
(4) Detach Interface Links
In this step the care must be taken to detach the management interfaces e.g. eno1, eno3, eno2 and eno4. So lspsci command should be used to find the management interfaces and not the additional 10G cards.

Proceed with guest creation using the virt command as indicated below:
The guest creation is explained using virsh command line utility, however user can also create VMs using the virtual machine manager utility, which is a GUI based tool.

1. Create VM

```
#    # virt-install --virt-type kvm --hvm --connect qemu:///system --host-device pci_0000_03_00_0,rom_bar=off --host-device pci_0000_03_00_1,rom_bar=off --cdrom /var/ORCL/TPD.install-7.6.2.0.0_88.58.0-OracleLinux6.10-x86_64.iso --disk path=/var/vm_server/VM_IMF_1A.disk,size=64,sparse=no,bus=ide --name VM_IMF_1A --autostart --boot cdrom,hd --ram 65536 --vcpus 92,cpuset=4-95 --graphics vnc --os-variant rhel6
```

2. The following arguments are to be provided to the virt-install command:

- Virtualization mode: --virt-type kvm --hvm --connect qemu:///system
- Network interfaces (keep the order):
  - Ethernet links detached from host: --host-device <*pci_device_id*>,rom_bar=off
- Boot order: --boot cdrom,hd
- CD drive: --cdrom <*TPD ISO File*>
- Disk: --disk path=<*disk_file*>,size=<*disk_size*>,sparse=no,bus=ide
- VM name: --name <*vm_name*>
- RAM: --memory <*ram_size*>
- CPU: --vcpus <*cpu_count*>,cpuset=<*cpu_set*>
- Display: --graphics vnc
- VM optimization: --os-variant rhel6

where

- <*TPD ISO File*> is the full path and name of the OL ISO file
- <*disk_file*> is the full path and name of the disk file (be sure to create it on a file system having enough space)
- <*disk_size*> is the size (in GB) of the disk to create
- <*vm_name*> is the name of the VM (preferably use letters, digits, underscores and hyphens)
  - <*ram_size*> is the size (in GB) of RAM to allocate to the VM; do not over allocate as the host itself and all of the guests will use RAM

<*cpu_count*> is the number of CPU to allocate to the VM; do not over allocate as the host itself and all of the guests will use CPU

3. After the IPM, the interfaces created on VM are eth0, eth1 and eth2 (this is created by default by KVM manager).

   Update the UDEV network file

   As root, on the VM:

   a. Check the configuration file 70-persistent-net.rules out:

      ```
      # rcstool co /etc/udev/rules.d/70-persistent-net.rules
      ```

   b. Rename the eth0 and eth1 to eth01 and eth03 and remove the eth2 device from this file (use vi to update the file)
   c. Check the configuration file 70-persistent-net.rules in:

      ```
      # rcstool ci /etc/udev/rules.d/70-persistent-net.rules
      ```

   Update the network configuration files

   As root, on the VM, repeat these steps for each network configuration file, namely ifcfg-eth0, ifcfg-eth1 and ifcfg-eth2:

   a. Move the ifcfg-eth0 and ifcfg-eth1 to ifcfg-eth01 and ifcfg-eth03 respectively and update the files to have the correct device name

      ```
      # mv /etc/sysconfig/network-scripts/ifcfg-eth<N> /etc/sysconfig/network-scripts/ifcfg-eth<xy>
      ```

   b. Update the DEVICE entry in the network configuration file ifcfg-ethxy to match the new name of the device; set the ONBOOT entry to no; remove a possible PERSISTENT_DHCLIENT entry (use vi to update the file)
   c. Enter the network configuration file ifcfg-ethxy in the version checking tool:

      ```
      # rcstool init /etc/sysconfig/network-scripts/ifcfg-eth<xy>
      ```

   Reconfigure udev and reboot

   As root, on the VM, follow the steps below:

   ```
   # udevadm control --reload
   ```

```
# udevadm trigger
# reboot
```

4. Shut down the VM and edit its configuration file to remove the default interface (eth2) created by KVM manager. This can be done by using virsh command line utiity.

```
# virsh shutdown VM_IMF_1A
# virsh edit VM_IMF_1A
# remove the entry for eth2 from the configuration file. Look for the “interface” tag and remove the tag from the domain xml file.
# Save the file.
# start VM_IMF_1A
```

5. Once more edit the /etc/udev/rules.d/70-persistent-net.rules file to remove the eth2 entry if created.

Integrated Acquisition Server application installation on guest

Note: Care must be taken for the bulkconfig file for the virtual IMF. Refer Appendix B for more information on the Acquisition server bulkconfig file format.

6. Provide the temporary IP address to the eth01.200 interface of the guest and copy the application ISO.
7. Refer to the section Install Acquisition Server Application for installing application.
8. After the IMF server installation is completed, verify the following on the IMF guest VMs
    - If **/etc/resolv.conf** file is present and it has nameserver entry e.g. nameserver 192.168.122.1. Then this entry should be commented out and **TKLCmf** service should be re-started

9. Refer to the section Configure Site and Subsystem for Acquisition Server for integration with CCM application and discovery of the sub-system on CCM.

Step 7: Mediation Server Guest Creation and Installation

The procedures in this section shall involve the mediation server guest creation. The section will also describe the procedure of OS re-installation on the guest.

For installation of each Mediation server, refer to the chapter Mediation guest creation and follow the chapter Mediation application installation procedures, after the guest has been created.

In order to create the Mediation guest or to reinstall the OS, the ISO file of the TPD used for IPM is needed on the host.

Mediation Guest Creation

Note: The guest creation is explained using virsh command line utility, however user can also create VMs using the virtual machine manager utility, which is a GUI based tool.

Refer steps from the section Mediation Guest Creation, to create the mediation server guests. Use only Backend bridge, however if the external production bridge is needed then adapt the command accordingly. Customize the hardware resources as needed on SUN X7-2 single guest.

After the guest is created and application is installed, integrate the server with CCM application using steps explained in chapters Integrate Customer Network and Add Mediation Subsystem to CCM. Make sure the JRE is already installed before discovering the acquisition sub-system on CCM.

The xDR Builders should be installed as next step after the mediation sub-system has been discovered on CCM. Follow steps mentioned in Install xDR Builders, to install xDR builders.

Mediation Guest OS reinstallation

Refer to the steps mentioned in section Mediation Guest OS reinstallation.

Mediation Server network device configuration

Refer steps from the section Mediation Guest network device configuration.

Multiple VM guests on the single hosts

Refer the table below for the hardware resource sharing for multiple VMs on SUNX7-2 server

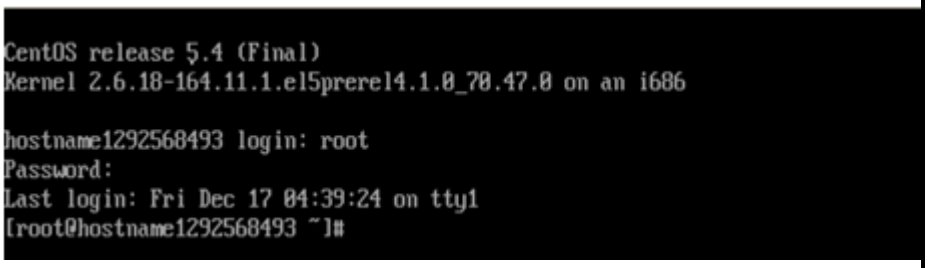
Function	vCPU	Minimum RAM	Minimum HDD	Configuration
Hypervisor	4	4	200 GB (*)	(*) This disk volume is what remains on the host
Mediation VM 1 (ixp1030-1a	23	62	150 GB	

Mediation VM 2 (ixp1030-1b	23	62	150 GB	
Mediation VM 3 (ixp1030-1c	23	62	150 GB	
Mediation VM 4 (ixp1030-1d	23	62	150 GB	

To create and install the guests VMs follow the procedures mentioned in Mediation Guest Creation. Customize the hardware resources for the VM as indicated in table Table 6.

Table 6: Hardware resources for the multiple mediation server guests

Appendix A: Manual configuration of Ethernet Interfaces

S T E P #	In this section you will be configuring the Ethernet interfaces in preparation to test them. You will be configuring the IP address, Netmask, Gateway for the interfaces on each TPD HP based server. If the final customer network and IP address information is not available at the time of this configuration, a default IP address for each server should be provided. **Prerequisites**: - The servers are loaded with TPD - The HP ProLiant servers will need to be connected to a KVM for access. Notes: Within the Platform Configuration Utility, the arrow and Tab keys on your keyboard can be used to move the cursor to different fields.	
1	Login to the server	Once the server completes the reboot from the ILO configuration process in the previous section, you should see a login prompt. Login as User: **root** and refer to TR006061 for the default "TPD root" password  **Expected Result:** Login prompt is displayed and you are logged in as root.

Using command line procedure

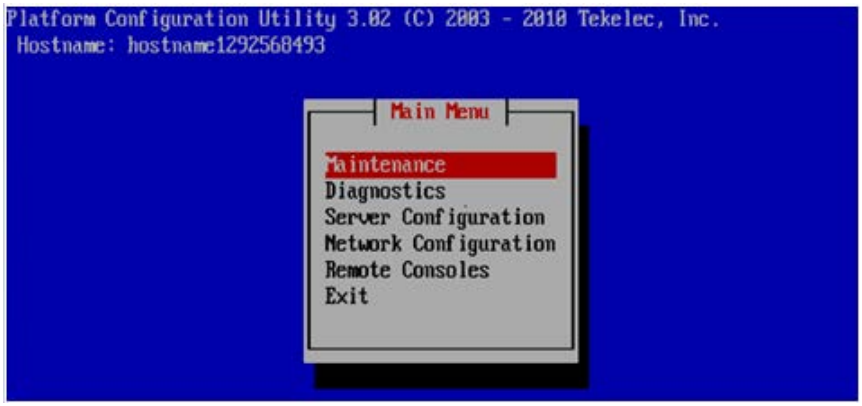
If you prefer to configure using the graphical interface skip this procedure and use the following platcfg menu procedure

2	Set the IP address and Netmask identified for the eth01 interface	**Command:** # ifconfig eth01 <***cust_IP_address***> netmask <***mask***> # **Expected Result:** No error after executing the command
3	Set the default Route Gateway IP address for the eth01 interface	**Command:** # route add default gw <***default_route_IP_address***> # **Expected Result:** No error after executing the command

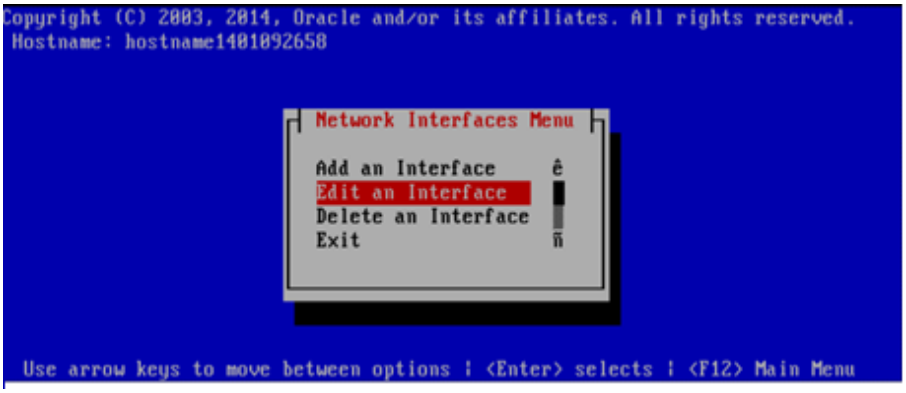
4	Configure remaining servers in frame	**Repeat Steps 1 through 3 for each equipped HP server.**

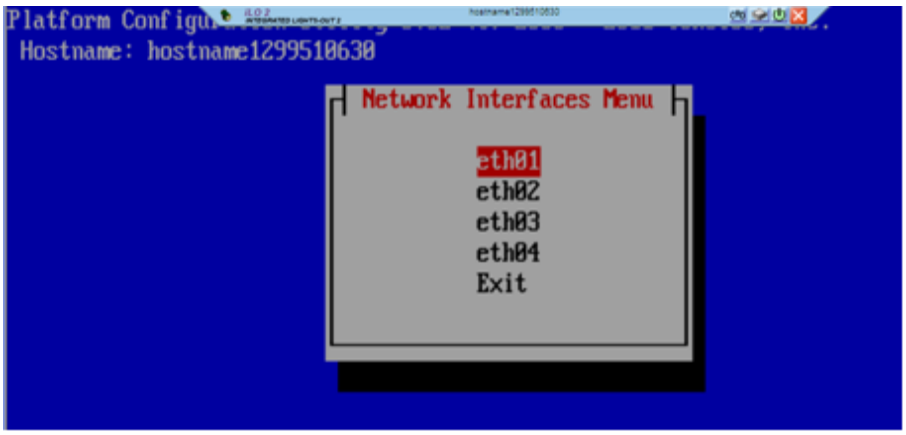
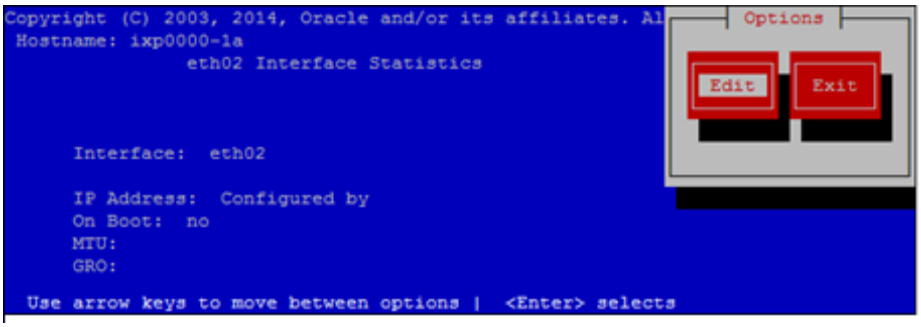
Using platcfg menu procedure

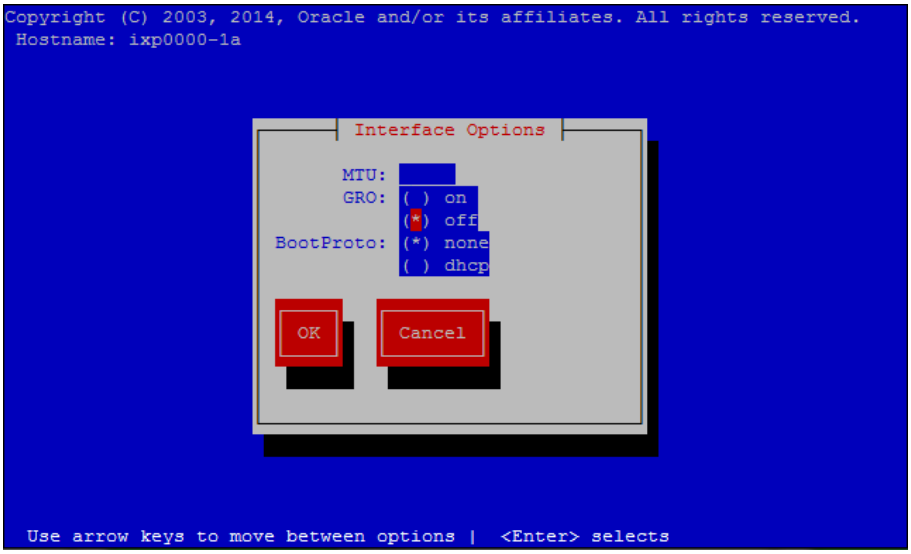
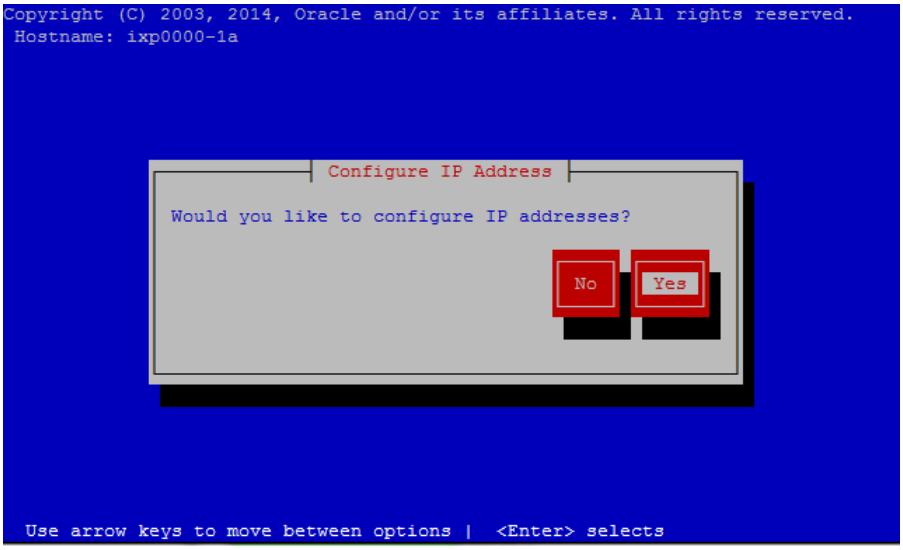
If you configures IP using the command line following the previous procedure, you can skip this procedure is already completed

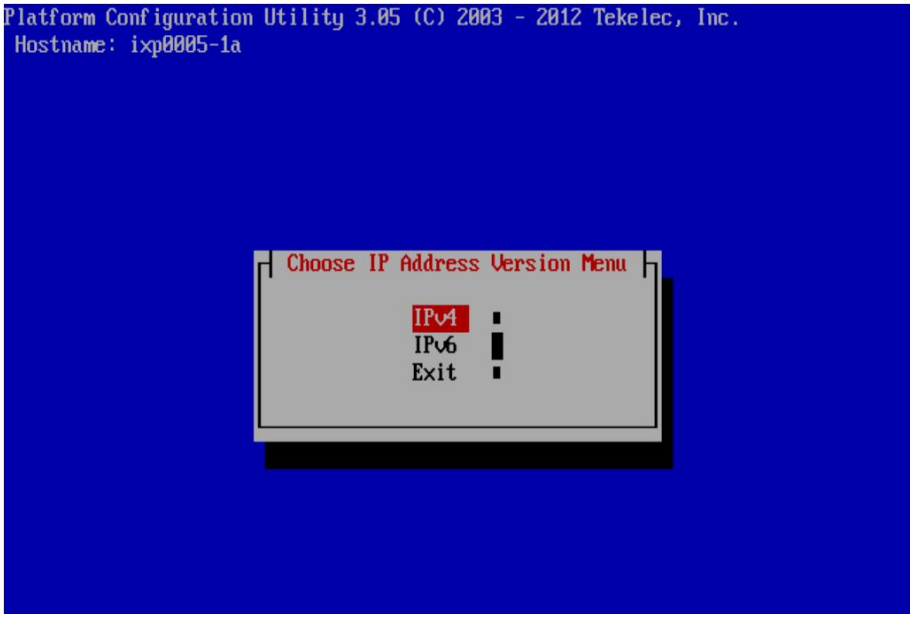
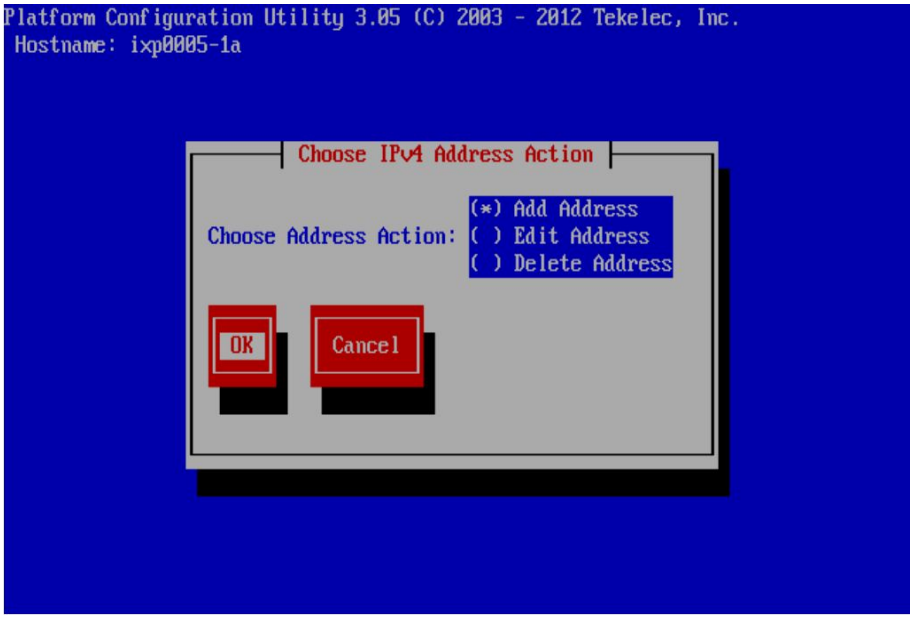
2	Enter the Platform Configuration Utility	To enter the Platform Configuration Utility menu enter: **su – platcfg** 
3	Enter the Platform Configuration Utility	 **Expected Result:** Main Menu of Platform Configuration Utility is displayed

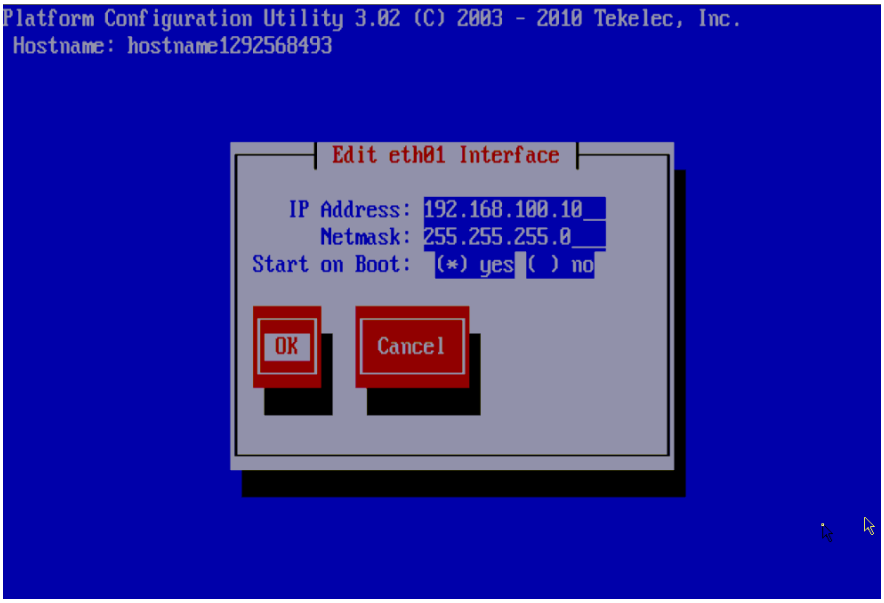
4	Enter the Network Configuration menu of the Platform Configuration Utility	Use the arrow keys on the keyboard to select **Network Configuration** and press [ENTER] to select it.  **Expected Result:** The Network Configuration menu is displayed
5	Enter the Network Interfaces menu	Use the arrow keys on the keyboard to select **Network Interfaces** and press **[ENTER]** to select it.  **Expected Result:** The Network Interfaces menu is displayed

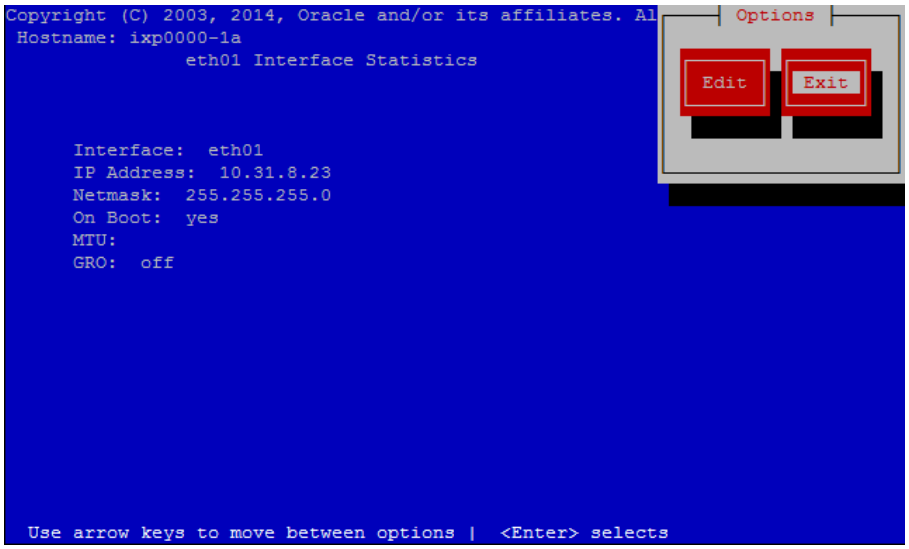
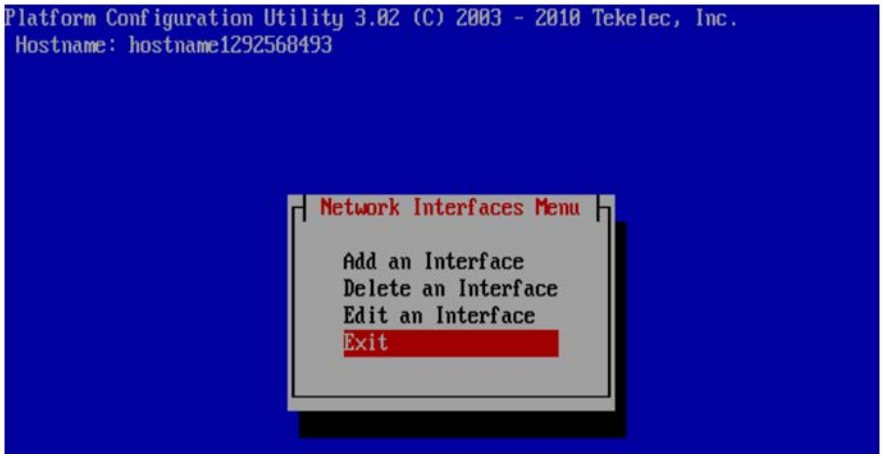
6	Enter the Edit an Interface menu	Use the arrow keys on the keyboard to select **Edit an Interface** and press **[ENTER]** to select it.  **Expected Result:** The Network Interfaces menu is displayed with interface choices eth01 and eth02

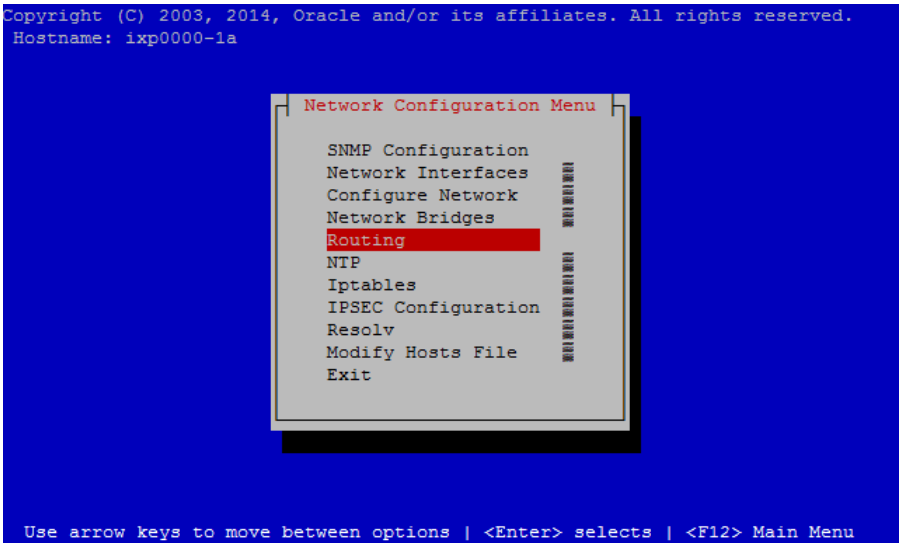
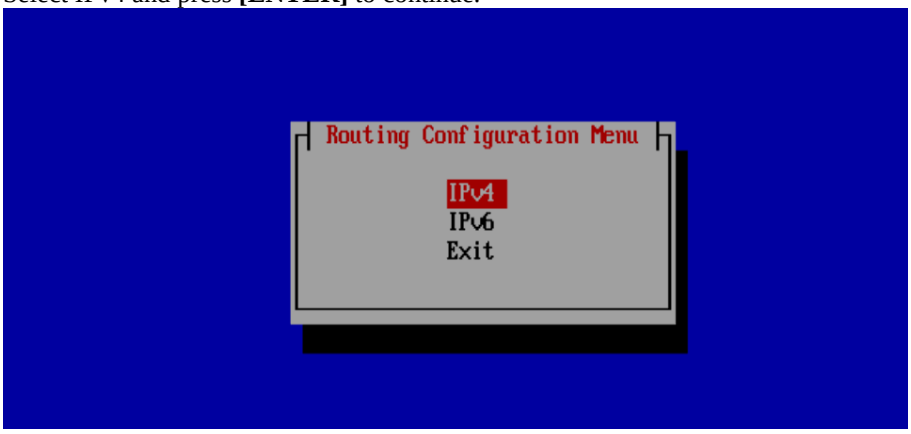
7	Edit the eth01 interface properties	Use the arrow keys on the keyboard to select **eth01** and press **[ENTER]** to select it.  **Expected Result:** The eth01 interface is selected and you are presented with **eth01 Interface Statistics**.  Press the **[ENTER]** key to Edit the properties of eth01. **Expected Result:** The eth01 interface is selected and you are presented with eth01 Interface Statistics. You have selected 'Edit' and are presented with properties to change.

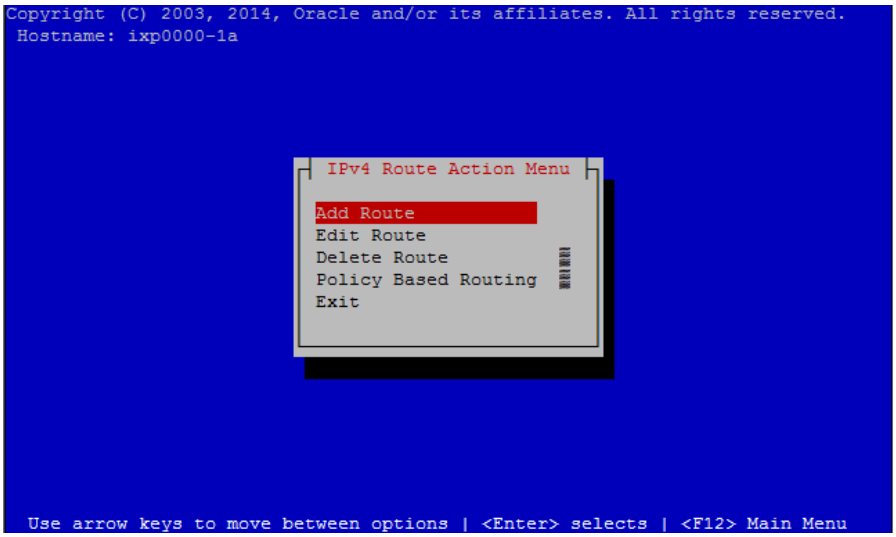
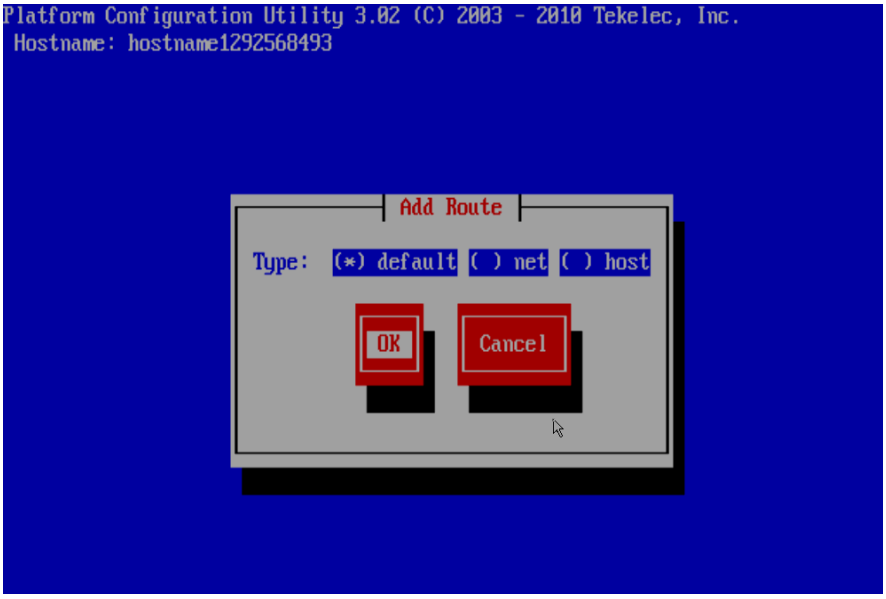
8	Configure MTU, GRO, and boot protocol	Press **[TAB]** to move to off for GRO, then press the **[SPACEBAR]** key to select it. An asterisk will appear once selected. Press **[TAB]** to move to OK, then press the **[ENTER]** key to continue.  **Expected Result:** GRO is set to off and you now see the menu which allows you to edit the IP address.
9	Configure IP	Press **[TAB]** to move to Yes, then press the **[ENTER]** key to continue. 

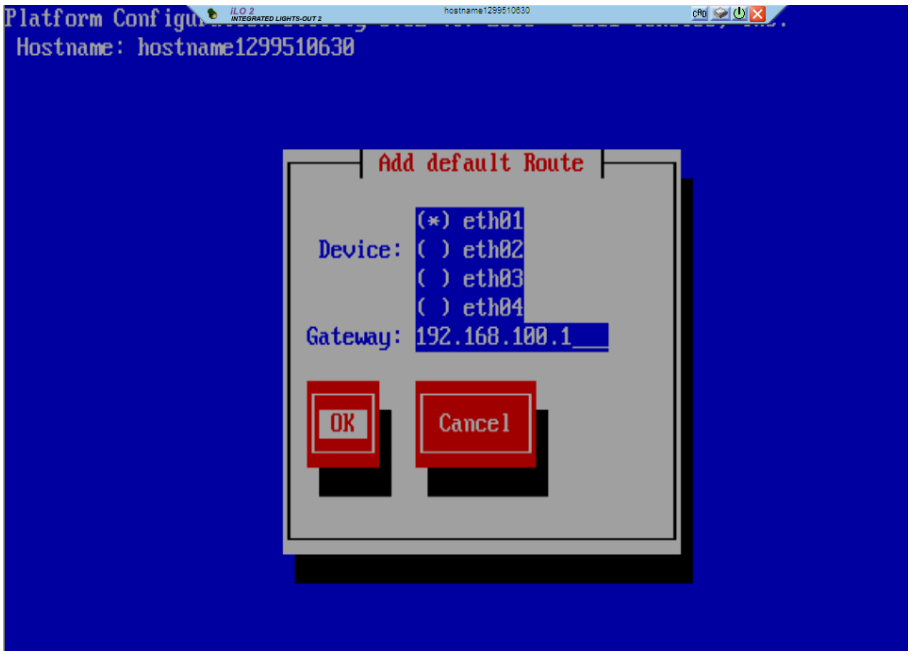
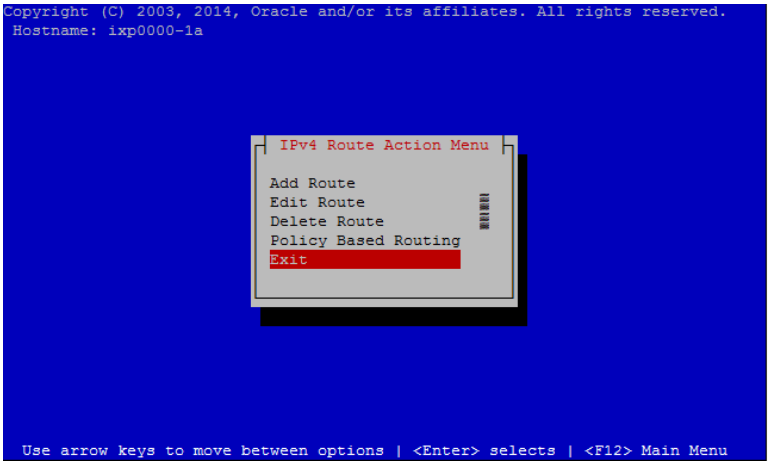
10	Select IPv4	press **[ENTER]** to continue. 
11	Select Add address	press **[ENTER]** to continue. 

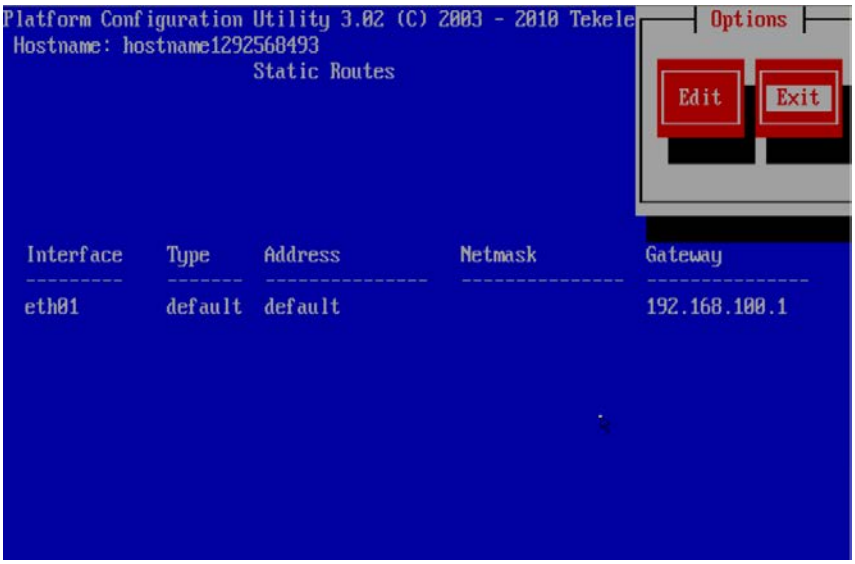
12	Set the IP address and Netmask identified for the eth01 interface	Use the **[TAB]** and arrow keys on the keyboard to add IP address. Enter the IP address of the server then press **[TAB]** to select NETMASK. Press **[TAB]** to select **( ) yes** and press **[SPACEBAR]** to select then **[TAB]** and press **[ENTER]** to continue. 
13		You will see the following screen:  **Expected Result:** IP address and Netmask is set to the correct IP address for the server. Wait for it to complete.

14	Verify the settings and exit	Once the screen comes back, **verify the IP address and Netmask**. Use the **[TAB]** key on the keyboard to select Exit and press **[ENTER]** to continue.  Use the **[TAB]** key on the keyboard to select Exit and press **[ENTER]** to continue  **Expected Result:** IP address and Netmask is set to the correct IP address for the server and you exit the Network Interfaces menu.

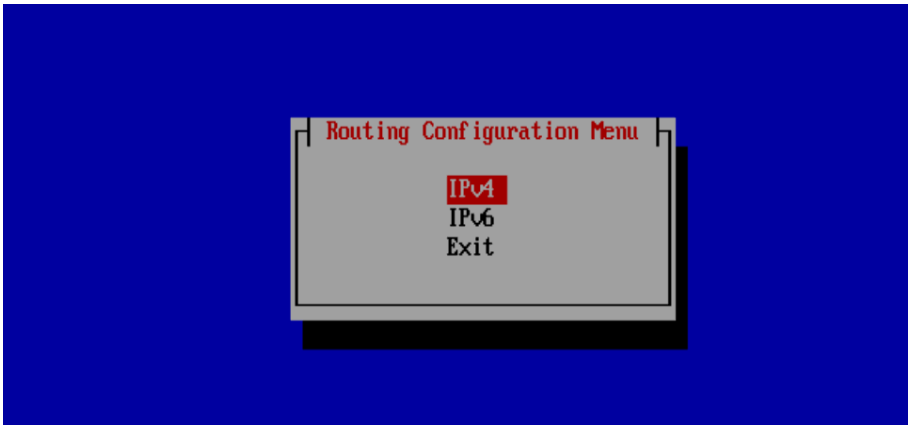
15	Set the Gateway address for the eth01 interface	Use the arrow keys on the keyboard to select Routing and press **[ENTER]** to continue.  Select IPv4 and press **[ENTER]** to continue.  Select Edit and press **[ENTER]** to add the default gateway.  **Expected Result:** Routing menu is opened and Edit is selected

16	Set the IP address and Netmask for the eth01 interface	Select Add Route using the arrow keys.  Use the **[TAB]** and **[SPACEBAR]** keys on the keyboard to select ( ) **default**, then **[TAB]** to **OK** and press **[ENTER]** to continue.  **Expected Result:** Default is selected and you are taken to the next menu which allows you to add the IP address of the default route.

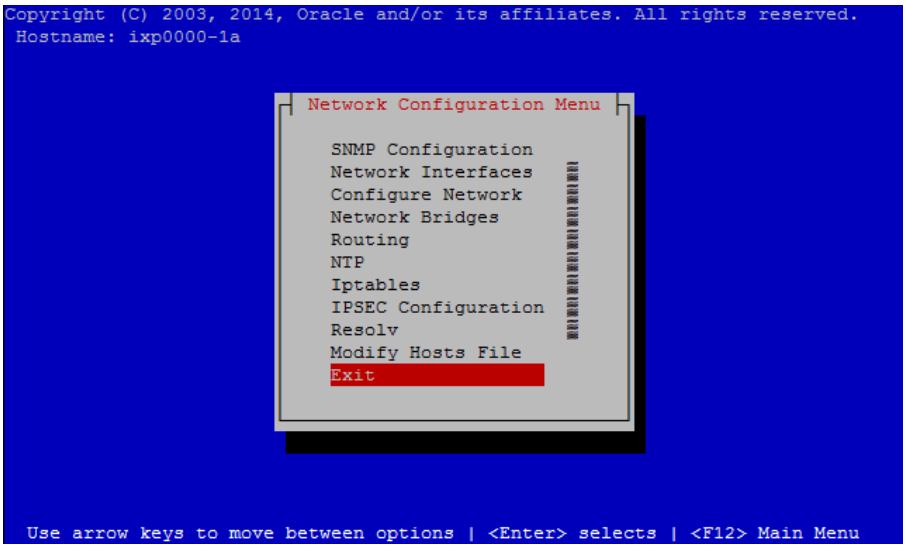
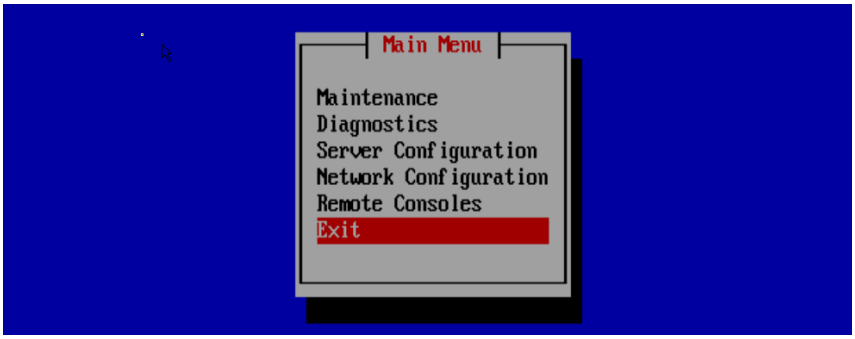
17	Set the default Route Gateway IP address for the eth01 interface	Use the **[TAB]** and **[SPACEBAR]** keys on the keyboard to select **( ) eth01** and then **[TAB]** twice and enter the correct customer's gateway IP address if available. If not available and you are using default test IP addresses instead, enter **192.168.100.1**. Press **[TAB]** to select **OK** then press **[ENTER]** to continue.  Use the arrow keys on the keyboard to select **Exit** then press **[ENTER]** to exit.  **Expected Result:** The correct Gateway IP address is entered. The Route Action menu is exited.
18	Verify the default Route for eth01 and exit the menu	Verify the **eth01** interface is listed and Type and Address are set to default. Gateway should match the IP address you entered in the previous step. Use the **[TAB]** key on the keyboard to select **Exit** and press **[ENTER]** to continue.



Select **Exit** and press **[ENTER]** to leave the **Routing Configuration** menu



Select **Exit** and press **[ENTER]** to leave the **Network Configuration** menu

		 Select **Exit** once again to leave the **Platform Configuration Utility**  **Expected Result:** The default route (Gateway) IP address is verified and the menu is exited.
19	Configure remaining servers in frame	Repeat Steps 1 through 18 for each equipped HP DL360 server.

Appendix B: Performance Intelligence Center Bulkconfig

Management Server Bulkconfig File Description

MGMT is installed on Standard Server and no bulkconfig file is required.

In case of TPD based platform use bulkconfig format as defined in PIC 10.1.5 Installation Guide

DRS Bulkconfig File Description

No bulkconfig file is required for a new DRS installation.

Mediation Server Bulkconfig File Description

The MEDIATION subsystem bulkconfig file contains the overall MEDIATION pre-installation configuration information.

Note: there is one bulkconfig file for each MEDIATION subsystem.

During the installation process, various scripts use this file to configure MEDIATION.

The bulkconfig file is a case sensitive text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The MEDIATION bulkconfig file template is located on the MEDIATION iso on the /upgrade/IXP_bulkconfig_template path. The file is unique for the MEDIATION subsystem and is present on each server in this subsystem.

Note: When you install Performance Intelligence Center, you are asked to create this bulkconfig file and update this file.

DO NOT remove the MEDIATION bulkconfig file from the server.

The MEDIATION subsystem bulkconfig file is used during these processes:

- Manufacturing installation
- Customer network integration
- Change IP
- Disaster recovery procedure

This topic provides a description of each keyword and parameter used in the bulkconfig file. It is

Important to read and understand the contents of this file.

Bulkconfig file location and rights

File name: bulkconfig

File absolute path: /root/bulkconfig

Mount the Mediation iso file. As root run:

```
# mount -o loop /var/TKLC/upgrade/iso_file.iso /mnt/upgrade
```

Copy the good bulkconfig file template:

```
# cp /mnt/upgrade/upgrade/IXP_bulkconfig_template /root/bulkconfig
```

Change the permission on the bulkconfig

```
# chmod 644 /root/bulkconfig
```

Unmount the MEDIATION iso file. As root run:

```
# umount /mnt/upgrade
```

Bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The

keyword is mandatory. Each line must begin with the keyword, and then contains various values for

this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,<hostname_of_1st_server>,<IP_address>,<function>,<interface_name>,<network_mask>,<network_gateway>
host,<hostname_of_2nd_server>,<IP_address>,<function>,<interface_name>,<network_mask>,<network_gateway>
...
host,<hostname_of_nth_server>,<IP_address>,<function>,<interface_name>,<network_mask>,<network_gateway>
ntpserver1,<IP_address>
ntpserver2,<IP_address>
ntpserver3,<IP_address>
ntppeerA,
ntppeerB,
nspprimary,<IP_address_of_first_weblogic_or_onebox_nsp_backend>
nspsecondary,<IP_address_of_secondary_weblogic>
nsporacle,<IP_address_of_oracle_server>
timezone,<time_zone>
pdu,<IP_address>,<directory_path>
...
```

The highlighted entries are for the PDU share directories on external storage server like ZFS

Refer to the following descriptions of each keyword and its associated values.

host Description

```
host,<hostname_of_1st_server>,<IP_address>,<function>,<interface_name>,<network_mask>,<network_gateway>
host,<hostname_of_2nd_server>,<IP_address>,<function>,<interface_name>,<network_mask>,<network_gateway>
...
host,<hostname_of_nth_server>,<IP_address>,<function>,<interface_name>,<network_mask>,<network_gateway>
```

Example (installation):

```
host,ixp1981-1a,10.336.2.141,IXP-PDU,eth01,255.255.255.224,10.336.2.129
```

```
host,ixp1981-1b,10.336.2.142,IXP-BASE,eth01,255.255.255.224,10.336.2.129
host,ixp1981-1c,10.336.2.143,IXP-BASE,eth01,255.255.255.224,10.336.2.129
```

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

Example (disaster recovery of ixp1981-1b server):

```
host,ixp1981-1a,10.336.2.141,IXP-PDU,eth01,255.255.255.224,10.336.2.129
host,ixp1981-1b,10.336.2.142,DR-BASE,eth01,255.255.255.224,10.336.2.129
host,ixp1981-1c,10.336.2.143,IXP-BASE,eth01,255.255.255.224,10.336.2.129
```

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

The host keyword has the following associated values:

hostname_of_nth_server the server hostname in the standard MEDIATION format: ixpNNNN-MA where:

- N is numeric 0-9
- M is numeric 1-9
- A is alphabetical a-z

IP_address The IP address of the server. For blade systems, the backend (VLAN 3) IP address of the server.

function The function of the server. Use one of the following entries for installation:

- IXP-PDU for the PDU Storage Server
- IXP-BASE for the IXP Base Server

Function for the disaster recovery procedure for the particular server is different. Use one of the following entries for disaster recovery:

- DR-PDU for the PDU Storage Server
- DR-BASE for the IXP Base Server

interface_name Name of the interface where the network settings are applied.

- eth01 for the rackmount systems
- bond0.3 for the blade systems

network_mask The network mask.

network_gateway The default gateway.

ntpserver Description

Refer to section How to configure NTP .

```
ntpserver1,<IP_address>
ntpserver2,<IP_address>
ntpserver3,<IP_address>
```

```
ntppeerA,
ntppeerB,
```

- ntpserver1 is the first NTP server
- ntpserver2 is the second NTP server
- ntpserver3 is the third NTP server
- ntppeerA not applicable; leave empty
- ntppeerB not applicable; leave empty

Example:

```
ntpserver1,10.336.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
```

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server.

NSP Description

```
nspprimary,<IP_address_of_first_weblogic_or_onebox_nsp_backend>
nspsecondary,<IP_of_secondary_weblogic>
nsporacle,<IP_address_of_oracle_server>
```

- nspprimary is the Management One-box Management server
- nsporacle is the Management Oracle server or Management Server One Box

Example:

```
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
```

The NSP keyword has the following associated values:

IP_address_of_primary_weblogic_or_onebox_nsp_backend The IP address of the MANAGEMENT SERVER server:

- One-box: backend IP address of the One-box Management Server

IP_address_of_secondary_weblogic The IP address of the Management Server:

- One-box: not applicable; leave empty

IP_address_of_oracle_server The IP address of the Management Server Oracle server:

- One-box: not applicable; leave empty

timezone Description

```
timezone,<time_zone>
```

Example:

```
timezone,Europe/Paris
```

The timezone keyword has the following associated value:

time_zone

The timezone string. For a list of available timezones that you can use, refer to the /usr/share/zoneinfo/zone.tab file TZ column. For example:

```
# cat /usr/share/zoneinfo/zone.tab
...
#code coordinates TZ comments
AD +4230+00131 Europe/Andorra
909-2122-001 Revision 1.11, February 02, 2012 DRAFT 210
PIC Bulkconfig File Description
AE +2518+05518 Asia/Dubai
AF +3431+06912 Asia/Kabul
AG +1703-06148 America/Antigua
CZ +5005+01426 Europe/Paris
...
```

bulkconfig file: installation example

A bulkconfig file needs to be created for the following MEDIATION subsystem:

- Subsystem hostname: ixp1981
- 1a server is the PDU Storage Server with the IP address: 10.336.2.141
- 1b server is the Base Server with the IP address: 10.336.2.142
- 1c server is the Base Server with the IP address: 10.336.2.143
- Network interface: eth01
- Network mask: 255.255.255.254
- Default gateway: 10.336.2.129
- NTP server IP address: 10.336.129.11
- NSP One-box IP address: 10.10.10.10
- Server timezone: Europe/Paris

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
# cat /root/bulkconfig
host,ixp1981-1a,10.336.2.141,IXP-PDU,eth01,255.255.255.224,10.336.2.129
host,ixp1981-1b,10.336.2.142,IXP-BASE,eth01,255.255.255.224,10.336.2.129
host,ixp1981-1c,10.336.2.143,IXP-BASE,eth01,255.255.255.224,10.336.2.129
ntpserver1,10.336.129.11
```

```
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
timezone,Europe/Paris
```

Automated records in /etc/bulkconfig file

During the automated integration of MEDIATION subsystem with EFS server(s) the following line is added to the /etc/bulkconfig file (one per integrated EFS server):

```
efs,<hostname_of_EFS>,<IP_address_of_EFS>
```

where

- hostname_of_EFS is the hostname of EFS that local DataFeeds hosts uses as an export target
- IP_address_of_EFS is the IP address of such EFS

Example:

```
efs,ixp7777-1e,10.336.0.33
```

External PDU storage server Description

After mediation server installation and before customer integration the following lines should be added in bulkconfig to add the mounts on external storage server for PDU storage.

```
pdu,<IP_address>,<directory_path>
...
```

- *pdu* is the keyword to identify the external pdu storage server entry.
- IP_address is the ip address of the external PDU storage server.
- directory_path is the path of directory on external PDU storage server to be mounted on mediation server to store the PDUs

Example for ZFS storage server :

```
pdu,10.31.2.72,/export/pdu_1
pdu,10.31.2.72,/export/pdu_2
pdu,10.31.2.75,/export/pdu_1
pdu,10.31.2.75,/export/pdu_3
```

Acquisition Server Bulkconfig File Description

This topic describes the syntax and use of the acquisition server bulkconfig file.

The acquisition server bulk configuration file contains the overall configuration information. The bulkConf.pl script uses this single file to configure the IMF subsystem or PMF accordingly.

The bulkconfig file is a text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The file is unique per subsystem and is present on each server in the subsystem.

DO NOT remove the acquisition server bulkconfig file from the server or subsystem.

This topic provides a description of each keyword and parameter used in the bulkconfig file (bulkconfig). It is important to read and understand the contents of this file.

Bulkconfig file location and rights

File name: bulkconfig

File path:/root/bulkconfig

Mount the Acquisition Server iso file. As root run :

```
# mount –o loop /var/TKLC/upgrade/iso_file.iso /mnt/upgrade
```

Copy the good bulkconfig file template:

```
# cp /mnt/upgrade/upgrade/XMF_bulkconfig_template /root/bulkconfig
```

Change the permission on the bulkconfig

```
# chmod 644 /root/bulkconfig
```

Unmount the Acquisition Server iso file. As root run :

```
# umount /mnt/upgrade
```

Bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

host,<***hostname_of_1st_server***>,<***IP_address***>,<***function***>,<***interface_name***>,<***network_mask***>,<***network_gateway***>,<***designation***>
host,<***hostname_of_2nd_server***>,<***IP_address***>,<***function***>,<***interface_name***>,<***network_mask***>,<***network_gateway***>,<***designation***>
...
host,<***hostname_of_nth_server***>,<***IP_address***>,<***function***>,<***interface_name***>,<***network_mask***>,<***network_gateway***>,<***designation***>
ntpserver1,<***IP_address***>
ntpserver2,<***IP_address***>
ntpserver3,<***IP_addres***>
ntppeerA,<***IP_address***>
ntppeerB,<***IP_address***>
nspprimary,<***IP_address_of_primary_nsp***>
nspsecondary,<***IP_address_of_secondary_nsp_appserver***>
nsporacle,<***IP_address_of_oracleDB_or_1Box***>
timezone,<***time_zone***>

xmf_install_mode***,OVS***

Refer to the following descriptions of each keyword and its associated values.

Host Description

host,<**hostname_of_1st_server**>,<**IP_address**>,<**function**>,<**interface_name**>,<**network_mask**>,<**network_gateway**>,<**designation**>
host,<***hostname_of_2nd_server***>,<***IP_address***>,<***function***>,<***interface_name***>,<***network_mask***>,<***network_gateway***>,<***designation***>
...
host,<***hostname_of_nth_server***>,<***IP_address***>,<***function***>,<***interface_name***>,<***network_mask***>,<***network_gateway***>,<***designation***>

Host Example for IMF Bare-metal setup:

host,imf-1a,192.168.253.5,IMF,bond0.200,255.255.255.224,192.168.253.1,1A
host,imf-1b,192.168.253.6,IMF,bond0.200,255.255.255.224,192.168.253.1,1B
host,imf-1c,192.168.253.7,IMF,bond0.200,255.255.255.224,192.168.253.1,1C

Host Example for virtual IMF as Pass-through setup:

host,imf-1a,192.168.253.5,IMF,bond0.200,255.255.255.224,192.168.253.1,1A
host,imf-1b,192.168.253.6,IMF,bond0.200,255.255.255.224,192.168.253.1,1B
host,imf-1c,192.168.253.7,IMF,bond0.200,255.255.255.224,192.168.253.1,1C

Host Example for virtual IMF as OVS setup:

host,imf-1a,192.168.253.5,IMF,eth2,255.255.255.224,192.168.253.1,1A
host,imf-1b,192.168.253.6,IMF,eth2,255.255.255.224,192.168.253.1,1B
host,imf-1c,192.168.253.7,IMF,eth2,255.255.255.224,192.168.253.1,1C

Example for PMF standalone:

host,pmf-0a,192.168.2.106,PMF,eth01,255.255.255.0,192.168.2.1,0A

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

The host keyword has the following associated values:

hostname_of_nth_server	The server hostname. Note: It is recommended that the hostname ends with the designation of the server (for example, malibu-1a).
function	The function of the server. Use one of the following entries: •he function

designation	The designation of the server is a combination of frame number and position of the server in the frame. Use the following rule: • IMF subsystem: 1A for the first server, 1B for the second server, etc. •F subsystem: 1A for
interface name	The name of customer network interface (typically: bond0.200 for IMF and eth01 for PMF)
IP_address	The IP address of the server. For blade systems, the internal IP address of the server
network_mask	The network mask
network_gateway	The default gateway

ntpserver Description

Refer to section How to configure NTP.

```
ntpserver1,<IP_address>
ntpserver2,<IP_address>
ntpserver3,<IP_addres>
ntppeerA,<IP_address>
ntppeerB,<IP_address>
```

- ntpserver1 is the first NTP server
- ntpserver2 is the second NTP server
- ntpserver3 is the third NTP server
- ntppeerA not applicable; leave empty
- ntppeerB not applicable; leave empty

Example:

```
ntpserver1,10.336.129.11
```

The ntpserver keyword has the following associated value:

IP_address	The IP address of the NTP server.

nsp Description

```
nspprimary,<IP_address_of_primary_nsp>
nspsecondary,<IP_address_of_secondary_nsp_appserver>
nsporacle,<IP_address_of_oracleDB_or_1Box>
```

- nspprimary is the management Primary server
- nspsecondary is the management Secondary WebLogic server
- nsporacle is the oracle database server. In case of 1box it will be same as nspprimary

Example (for a One-box Management Server):

```
nspprimary,10.10.10.10
```

The nsp keyword has the following associated values:

IP_address_of_primary_nsp The IP address of the Management Server Primary server:

- One-box: backend IP address of the One-box Management Server

IP_address_of_secondary_nsp The IP address of the Management Server Secondary server:

- One-box: not applicable; leave empty

timezone Description

```
timezone,<time_zone>
```

Example:

```
timezone,Europe/Paris
```

The timezone keyword has the following associated value:

time_zone The timezone string. For a list of available timezones that you can use, refer to the /usr/share/zoneinfo/zone.tab file **TZ** column. For example:

```
# cat /usr/share/zoneinfo/zone.tab
...
#code      coordinates          TZ                  comments
AD                    +4230+00131      Europe/Andorra
AE                    +2518+05518      Asia/Dubai
AF                    +3431+06912      Asia/Kabul
AG                    +1703-06148      America/Antigua
CZ                    +5005+01426      Europe/Prague
...
```

Xmf_install_mode Description

```
xmf_install_mode,<mode>
```

Example:

```
xmf_install_mode,OVS
```

The xmf_install_mode keyword has the following associated values **OVS** or **PASSTHRU.** This parameter is only used for virtual IMF installation to distinguish between OVS mode or PASSTHRU mode. This parameter is not required for bare-metal IMF and for PMF (either virtualized or bare-metal)

Bulkconfig file: example

A bulkconfig file needs to be created for the following acquisition server subsystem:

- Subsystem hostname: imf-1a
- 1a server with the IP address: 192.168.253.5
- 1b server with the IP address: 192.168.253.6
- 1c server with the IP address: 191.168.253.7
- IMF subsystem, interface: bond0.200
- Network mask: 255.255.255.224
- Default gateway: 192.168.253.1
- NTP server IP address: 10.350.32.10
- Subsystem is added to the appserver with IP address: 10.10.10.10
- Subsystem timezone: Europe/Paris

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

Sample bulkconfig file for IMF in bare-metal

```
# cat /root/bulkconfig
host,imf-1a,192.168.253.5,IMF,bond0.200,255.255.255.224,192.168.253.1,1A
host,imf-1b,192.168.253.6,IMF,bond0.200,255.255.255.224,192.168.253.1,1B
host,imf-1c,192.168.253.7,IMF,bond0.200, 255.255.255.224,192.168.253.1,1C
ntpserver1,10.350.32.10
ntpserver2,10.350.32.11
ntpserver3,10.350.32.12
ntppeerA,10.350.32.13
ntppeerB,10.350.32.14
nspprimary,10.10.10.10
nspsecondary,10.10.10.11
nsporacle,10.31.2.60
timezone,Europe/Paris
```

Sample bulkconfig file for virtual IMF in Pass-through

```
cat /root/bulkconfig
host,imf-1a,192.168.253.5,IMF,bond0.200,255.255.255.224,192.168.253.1,1A
host,imf-1b,192.168.253.6,IMF,bond0.200,255.255.255.224,192.168.253.1,1B
host,imf-1c,192.168.253.7,IMF,bond0.200, 255.255.255.224,192.168.253.1,1C
ntpserver1,10.350.32.10
ntpserver2,10.350.32.11
ntpserver3,10.350.32.12
ntppeerA,10.350.32.13
ntppeerB,10.350.32.14
nspprimary,10.10.10.10
nspsecondary,10.10.10.11
nsporacle,10.31.2.60
timezone,Europe/Paris

xmf_install_mode,PASSTHRU
```

Sample bulkconfig file for virtual IMF in OVS mode

```
cat /root/bulkconfig
host,imf-1a,192.168.253.5,IMF,eth2,255.255.255.224,192.168.253.1,1A
host,imf-1b,192.168.253.6,IMF,eth2,255.255.255.224,192.168.253.1,1B
host,imf-1c,192.168.253.7,IMF,eth2,255.255.255.224,192.168.253.1,1C
ntpserver1,10.350.32.10
ntpserver2,10.350.32.11
ntpserver3,10.350.32.12
ntppeerA,10.350.32.13
ntppeerB,10.350.32.14
nspprimary,10.10.10.10
nspsecondary,10.10.10.11
nsporacle,10.31.2.60
timezone,Europe/Paris

xmf_install_mode,OVS
```

Appendix C: Procedures

Change Customer Icon (Optional)

This procedure describes how to change the customer icon (for example, replace the default logo with a customer logo). This procedure is optional.

1. Open a terminal window and log in as oracle on Management server.
2. Copy the customer icon file (customer_icon.jpg) to the /opt/www/nsp/resources directory.
3. Verify the customer icon properties:

   The file name must be customer_icon.jpg.

   The file must belong to user oracle in group install.

   The compression format must be Jpeg.

   Optimum width/height ratio is 1.25.

   Any image can be used; the suggested minimum width/height is 150 pixels.

Install Optional Applications

This procedure describes how to install the optional applications:

- L99465 PIC Mediation DataFeed.sh
- L99467 PIC Multiprotocol Troubleshooting Application.sh
- L99468 PIC Network and Service Alarm Applications.sh
- L99469 PIC Network and Service Dashboard.sh
- L99470 PIC SS7 Network Surveillance Applications.sh
- L99471 On Demand User Plane Capture Application.sh
- Session Point Code

The steps are:

1. Open a terminal window and log in as tekelec on the Management Admin server.
2. Change directory to /opt/nsp/nsp-package/framework/install/dist/install/optional/exec folder
3. Install the required optional application by running the corresponding executable for that application.

   For example : To install optional application “PIC Network and Service Dashboard.sh“ type the name of script “sh L99469_PIC_Network_and_Service_Dashboard.sh” and hit enter command
4. The install logs are available at /var/log/nsp/install/activate_optional.log.

Configure Purchased Tokens

This procedure describes how to increase purchased tokens after Management server installed

1. Open a terminal window and log in as tekelec on the Management server.
2. Change dir to /opt/nsp/nsp-package/framework/install/dist/install/optional/exec folder
3. Run the script “sh L99466_PIC_Management_Application.sh” provided. It will prompt for number of concurrent users (the number of purchased tokens). Enter the value.

   Note: that number of tokens cannot be decreased and its maximum value is 50 only.
4. After the value provided it will successfully increase the token.

Capacity Management KPI configurations

Refer to 10.4.0 Maintenance Guide for **Capacity Management Good Practices.**

How to configure NTP

NTP architecture

Configure two OCPIC servers as NTP servers taking in account the préférence described below.

On these servers NTP configure one or more customer NTP and the second OCPIC NTP as a peer. (see platcfg screenshot below). Make sure each OCPIC NTP are connected to “independent” NTP and don’t share the customer NTP servers.

On all other servers use these OCPIC NTP as ntpserver1 and ntpserver2. (Figure 8)

Don’t configure the customer NTP as backup of the OCPIC NTP you selected!

If there are remote site(s) with poor NTP synchronization use some local servers as OCPIC NTP. This is especially the case when you have Acquisition server or Mediation server installed on site in different regions from a big country and using a single Management Server.

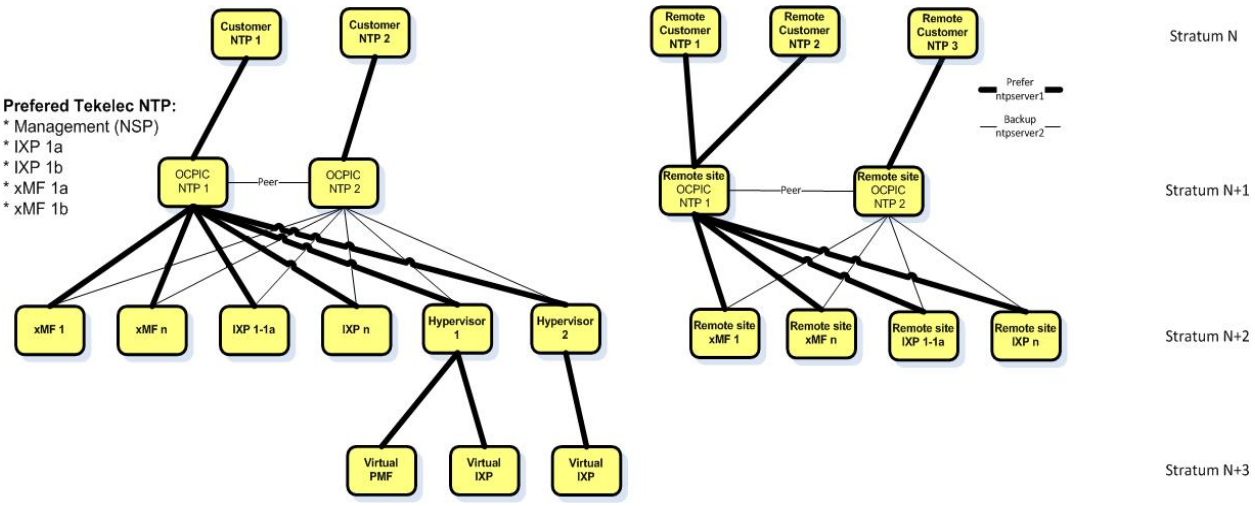


Figure 8: Acquisition server or Mediation server installed on site in different regions from a big country and using a single Management Server

Reminder: NTP setup is operated by bulkconfig file on a Tekelec Platform Distribution based server and according to MOS note 2218323.2 on a standard server.

Check the NTP precision

Wait sometime after the configuration and check the NTP using the command ntpq -p on each server

```
[cfguser@ixp0051-1z ~]$ ntpq -p
remote refid st t when poll reach delay offset jitter
==============================================================================
*ntpserver1 10.16.0.2 3 u 1 16 377 0.180 1.013 0.023
+ntpserver2 192.5.41.41 2 u 1 16 377 0.292 9.233 0.044
+ntpserver3 192.5.41.41 2 u 2 16 377 0.264 1.108 0.064
```

Results are in milliseconds.

ntpstat summarize the status of ntp:

```
[root@ixp0001-1a ~]# ntpstat
synchronised to NTP server (10.2.7.7) at stratum 5
time correct to within 171 ms
polling server every 64 s
```

Analyze results of ntpdc -nc peers:

Remote	Local	St	Poll	Reach	Delay	Offset	Disp
*10.31.1.208	10.30.2.111	1	32	377	0.00021	-0.000019	0.00032

- **Remote**: The remote host name or Internet address of a peer or server of the responding host. The character in the left margin indicates the mode this peer entry is operating in:
  - + indicates symmetric passive
  - = means the remote server is being polled in client mode
  - ^ indicates that the server is broadcasting to this address
  - ~ denotes that the remote peer is sending broadcasts
  - * marks the peer the server is currently synchronizing to

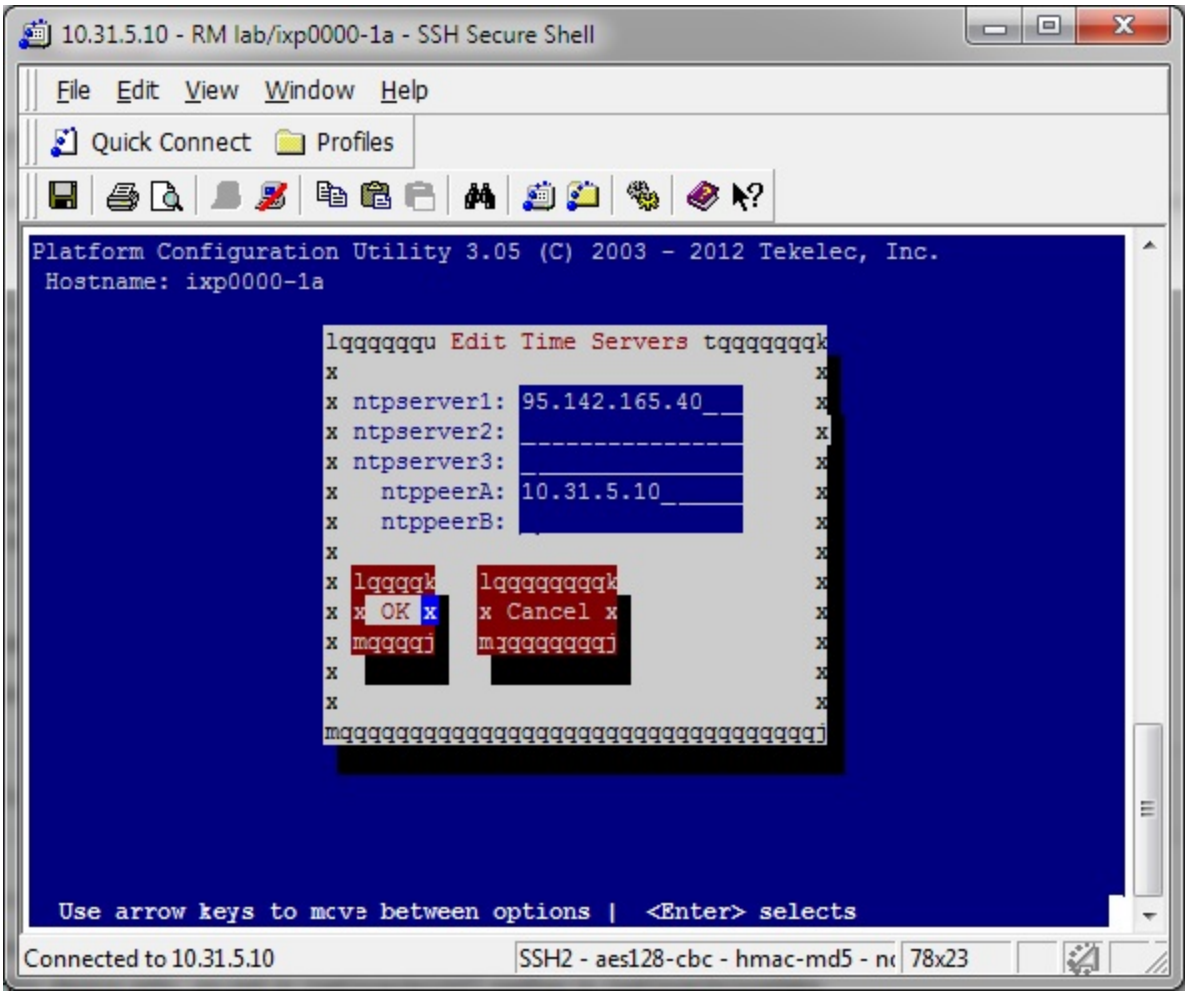
- **Local**: The Internet address of the responding host that was specified on the ntpdc command line.
- **St < 16** : The current operating stratum level of the peer or server. Since the NTP hierarchy can change dynamically the stratum levels may change. Lower stratum levels correspond to fewer hops to an accurate time source, and do not necessarily correspond to higher accuracy.
- **Poll**: Current polling interval in seconds for this peer or server. Polling intervals change dynamically.
- **Reach**: Reachability in response to the last 8 polls (value of 8-bit shift register). A value of 0377 indicates the remote system responded to the last 8 polls.
- **Delay**: The estimated round-trip delay in milliseconds for NTP message exchanges between the responding host and this peer or server. Delay is calculated from the previous 8 polls. Should be bellow 10 ms.
- **Offset**: The estimated offset between the peer or server's time and the responding host's time in milliseconds. This value is calculated from the previous 8 polls. Should be bellow 1 ms.
- **Disp**: The current estimated value of dispersion in milliseconds for this peer's offset/delay pair. Dispersion is used by the ntpd daemon in the clock selection algorithm. Increasing values of dispersion are associated with decreasing quality of the estimate.

You should not hesitate to wait few minutes and to launch again the command; numbers should evolve.

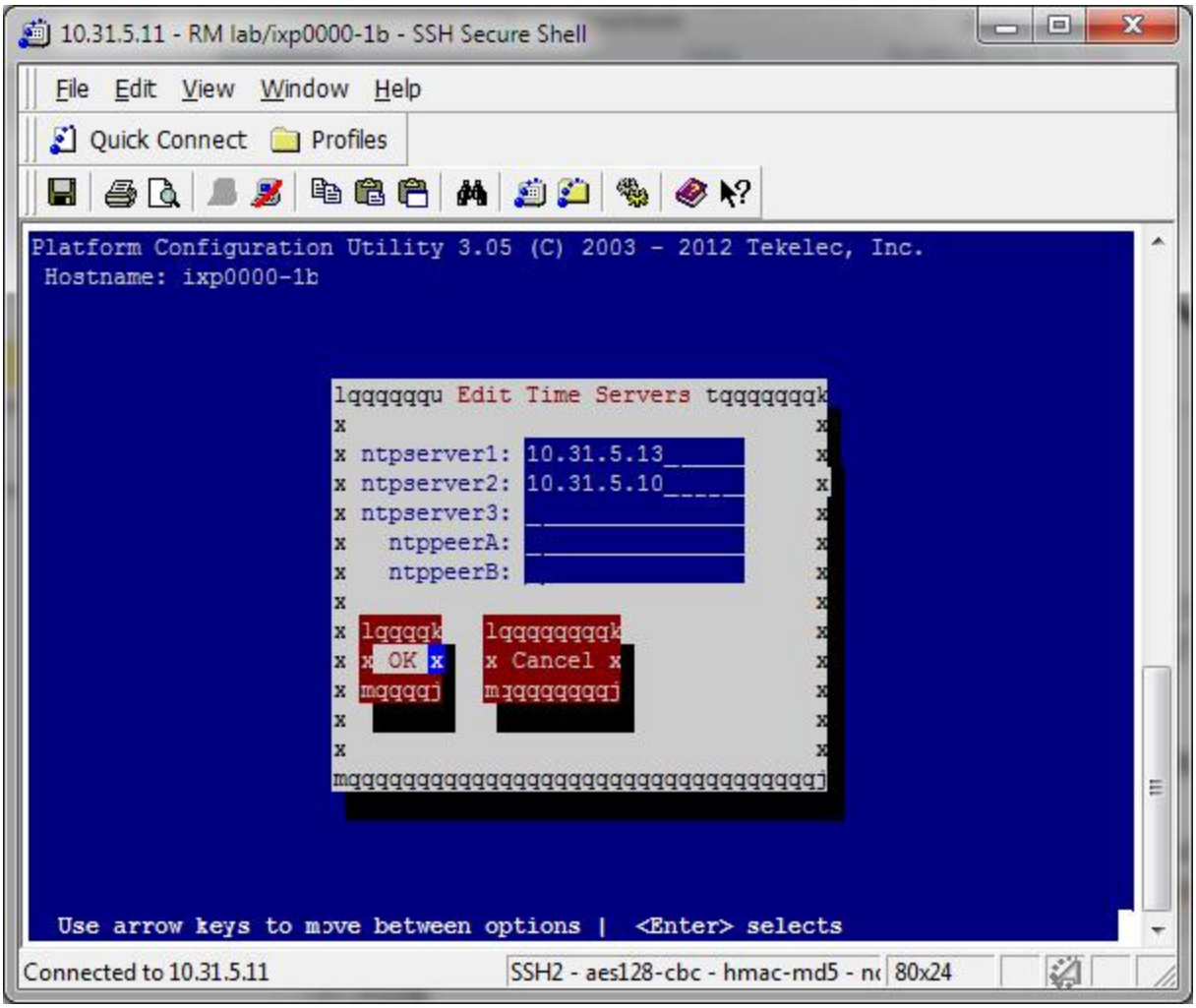
If you have an error on the command, it means that the service ntpd is not started. One can start again the service NTP by using the command service ntpd restart . Be careful, that should start again the NTP service, but that does not mark it in automatic restarting. If the service is not configured in automatic starting in the Linux services, after a rebooting of the PC, the service will be stopped.

Results in seconds.

Server used as OCPIC NTP server configuration



Other server sync on OCPIC NTP server configuration



Sync Database Credentials

The procedure is needed to be executed in following scenarios:

- A new server is added into an Acquisition Subsystem
- A new server is added into a Mediation Subsystem

1. Log on to management server as root user.
2. Execute below commands

```
# su - tekelec
# cd /opt/nsp/scripts/oracle/cmd/
# sh syncFiles.sh
```

or

```
# sh syncFiles.sh <IP1>
```

or

```
# sh syncFiles.sh <IP1> <IP2> ... <IPn>
```

The script if not provided any argument shall perform the sync of credentials to all the server discovered in various sites managed by the management server.

If the script is executed with one or more IP address (separated by space), then credentials shall be synced to all the IP address passed as arguments.

Note: During the execution, the script will ask for the root password of mgmt. server and cfguser password of target server for synching credentials with mediation and acquisition servers discovered in the various sites managed on this management server. The password for cfguser user shall be asked only for the server(s) on which the ssh keys are not already shared between tekelec and cfguser.

Modify Wallet Password

The procedure should be executed in case user want to modify the password for wallet.

1. Log on to management server as root user.
2. Execute below commands

```
# cd /opt/nsp/scripts/oracle/cmd
# ./modifyPassword.sh WALLET
```

The script shall prompt for the following:

- The old password: the existing wallet password.
- The new password: the new wallet password.

Note: During the execution, the script will ask for the root password of management server and cfguser password of target server for synching credentials with mediation and acquisition servers discovered in the various sites managed on this management server. The password for cfguser user shall be asked only for the server(s) on which the ssh keys are not already shared between tekelec and cfguser.

Modify Database Password

The procedure is needed to be executed in following scenarios:

- Password Change of Management Database user
- Password Change of Data Record Storage Database user
- Adding a new Data Record Storage Server in an existing site or a new site
- After Major upgrade to 10.3, so that wallet for database user is generated and sync to various susbsystem(s)

1. Log on to management 1box as root user.
2. Execute below commands

```
# cd /opt/nsp/scripts/oracle/cmd/
# sh modifyPassword.sh
```

The script will ask for below parameters:

- Database User Name e.g. “NSP” for management database or “IXP” for Data Record Storage Server database
- Service Name e.g. “NSP” for management database or “IXP” for Data Record Storage Server database
- Database Server IP Address : IP Address of the server where the database is hosted.

- Old Password of database user
- New Password to be set: It can be same as old but the script shall warn the user for new and old password being same.
- Confirmation of new password
- Wallet Password: Take the wallet password from database administrator
- Password of "sys" user : Take the sys user password from database administrator

In case the user wishes to modify the database user profile then section "**Modification of the user Profile in Database**" can be referred from the OCPIC 10.3 Maintenance Guide

Note: Follow the Oracle Secure password guidelines for setting up the database password. The password may only contain special characters from # ! % ^ & * ( ) _ + - { } [ ] ; : . , < > ? ~. This is only applicable for the NSP and IXP user.

Note: During the execution, the script will ask for the root password of mgmt. server and cfguser password of target server for synching credentials with mediation and acquisition servers discovered in the various sites managed on this management server. The password for cfguser user shall be asked only for the server(s) on which the ssh keys are not already shared between tekelec and cfguser.

Mediation Subsystem Healthcheck

This procedure describes how to run the automatic healthcheck of the Mediation subsystem.

1. Open a terminal window and log in on any Mediation server in the Mediation subsystem you want to analyze.
2. As **cfguser**, run:

```
$ analyze_subsystem.sh
```

The script gathers the healthcheck information from all the configured servers in the subsystem. A list of checks and associated results is generated. There might be steps that contain a suggested solution. Analyze the output of the script for any errors. Issues reported by this script must be resolved before any further use of this server.

The following examples show the structure of the output, with various checks, values, suggestions, and errors.

Example of overall output:

```
$ analyze_subsystem.sh
-----------------------------------------------------
ANALYSIS OF SERVER ixp0907-1a STARTED
-----------------------------------------------------

09:39:25: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
09:39:25: date: 05-17-15, hostname: ixp0907-1a
09:39:25: TPD VERSION: 7.0.1.0.0-86.20.0
09:39:26: IXP VERSION: [ 10.1.5.0.0-3.2.0 ]
09:39:26: XDR BUILDERS VERSION: package TKLCxdrbuilders is not installed
09:39:27: -----------------------------------------------
09:39:27: Analyzing server record in /etc/hosts
09:39:28:         Server ixp0907-1a properly reflected in /etc/hosts file
09:39:28: Analyzing IDB state
09:39:29:         IDB in START state
09:39:29: Analyzing shared memory settings
09:39:30:         Shared memory set properly
09:39:30: Analyzing IXP Licence
09:39:31:         Ixp Licence Valid
09:39:31: Analyzing mount permissions
```

```
09:39:32:       Writing enabled for pdu_1
09:39:32:       Writing enabled for pdu_2
09:39:33:       All mount permissions set properly
09:39:33: Analyzing date
09:39:33:       NTP deamon is running
09:39:34:       IP of NTP server is set
09:39:34: Checking CPU usage
09:39:34:       CPU usage check done
09:39:35: Running iaudit
09:39:36:       iaudit did not find any errors
09:39:37: Analyzing synchronization of server
09:39:38:       Role of server is StbMaster
09:39:38:       ActMaster server - ixp0907-1b
09:39:39:       StbMaster server - ixp0907-1a
09:39:40:       Server synchronizating properly
09:39:40: Analyzing NSP servers settings
09:39:41:       nsp_primary reflected in /etc/hosts
09:39:41:       Ping to nsp_primary OK
09:39:42:       nsp_secondary reflected in /etc/hosts
09:39:42:       Ping to nsp_secondary OK
09:39:42:       nsp_oracle reflected in /etc/hosts
09:39:43:       Ping to nsp_oracle OK
09:39:43:       Oracle on nsp_oracle accessible
09:39:44: Analyzing disk usage
09:39:44:       Space not exceeded
09:39:45: Analyzing JMX agent properties
09:39:45:       Instance ID of JMX agent OK
09:39:47:       IxpMbean [ application type IXP+2 ] located
09:39:47: Checking syscheck - this can take a while
09:39:49:       No active alarms
09:39:50: Checking services
09:39:50:       NFS service is running
09:39:51:       Portmap service is running
09:39:51: Analyzing ssh keys
09:39:51:       Ping to ixp0907-1a OK
09:39:52:       Ping to ixp0907-1b OK
09:39:52:       Ping to ixp0907-1c OK
09:39:52:       Ping to ixp0907-1d OK
09:39:53:       All keys for cfguser accounts exchanged
09:39:53: Analyzing DaqServer table in IDB
09:39:54:       Server ixp0907-1a reflected in DaqServer table
09:39:55:       Server ixp0907-1b reflected in DaqServer table
09:39:55:       Server ixp0907-1c reflected in DaqServer table
09:39:56:       Server ixp0907-1d reflected in DaqServer table
09:39:58:       VIP is set in DaqSubSystem table
09:39:59:       VIP is set in HaVipDef table
09:39:59:       Ping to 10.350.70.115 OK
09:40:00:       VIP is accessible
09:40:00: Analyzing processes
09:40:29: >>> Error: There are too many Dataflow processings (18). Should be 10 at most
09:40:29: >>> Suggestion: Dataflows should be redistributed to other servers
09:40:30:       Processes analysis done
09:40:30: Analyzing Data Feed status
09:40:31:       Data Feed analysis OK
```

```
09:40:31:           pdu_1 found in /etc/exports
09:40:32:           pdu_2 found in /etc/exports
09:40:32: Analyzing bulkconfig content
09:40:33:           BulkConfig content is consistent
09:40:33: All tests passed!
09:40:33: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp0907-1a

-----------------------------------------------------
ANALYSIS OF SERVER ixp0907-1b STARTED
-----------------------------------------------------

...

ixp0907-1a      TPD: [ 7.0.1.0.0-86.20.0 ]      IXP: [ 10.1.5.0.0-3.2.0 ]       XB: None            0 test(s) failed
ixp0907-1b      TPD: [ 7.0.1.0.0-86.20.0 ]      IXP: [ 10.1.5.0.0-3.2.0 ]       XB: [ 10.1.5.0.0-3.2.0 ]        0
test(s) failed
ixp0907-1c      TPD: [ 7.0.1.0.0-86.20.0 ]      IXP: [ 10.1.5.0.0-3.2.0 ]       XB: [ 10.1.5.0.0-3.2.0 ]        0
test(s) failed
ixp0907-1d      TPD: [ 7.0.1.0.0-86.20.0 ]      IXP: [ 10.1.5.0.0-3.2.0 ]       XB: [ 10.1.5.0.0-3.2.0 ]        0
test(s) failed
```

Example of a failed test:

```
12:21:48: Analyzing IDB state
12:21:48: >>> Error:    IDB is not in started state (current state X) 12:21:48: >>> Suggestion: Verify system stability and
use 'prod.start' to start the product
```

Disable Eth04 on E-5APP-B

It has been observed that on E-5APP-B server, eth04 interface logs a lot of traces in /var/log/messages that makes troubleshooting difficult. To overcome this issue following workaround should be applied.

1. As root user execute,

```
# ifdown eth04
```

2. Verify if eth04 is down using ifconfig, the state of interface should not be up

```
# ifconfig eth04
```

3. Disable OnBoot property for eth04

```
# su - platcfg
Go to Network Configuration->Network Interfaces
Select eth04 and edit to update the DHCP options.
Modify OnBoot to “NO”
Save and Exit
```

JRE Installation

JRE has to be installed separately, post application installation, on Acquisition and Mediation servers.

The minimal supported JRE release is “1.8.0”. The following instruction must be executed on all the mediation and acquisition servers before integration with management server.

1. Follow the MOS KM 1412103.2 to download the latest version of JRE 1.8.0:
   - In the section “Downloads (Latest JDK/JRE)”, click on JDK/JRE 8
   - On the next page, be sure to choose the platform “Linux x86-64”, then start the downloading
   - The downloaded file is an archive containing several other files: extract the file called jre-8u*XXX*-linux-x64.rpm, where *XXX* is the build number

   For example, by November 2016, the following files are available:
   - p18143322_1800_linux-x86-64.zip is the downloaded archive
   - jre-8u**112**-linux-x64.rpm is the package to install (one of the files of the archive)

2. Copy the package file on the server at /var/TKLC/upgrade

3. Install the JRE package, as root:

```
# cd /var/TKLC/upgrade
# rpm -Uvh <jre_rpm>
```

   Provide the name of the package file to install.

4. Keep the package safe from a possible incremental upgrade of the server, as root:

```
# su - platcfg
```

   a. Browse to **Maintenance → Upgrade → Non Tekelec RPM Management**
   b. Do **Add Non Tekelec RPMs to TPD control** for the JRE package. Ignore all other packages.
   c. Check that the package is under TPD control, by selecting **List Non Tekelec RPMs under TPD control**.
   d. Leave the platcfg menu.

5. Restart the java processes, as cfguser:

   On **Acquisition Servers**:

```
# pm.set off jmxAgent; pm.set on jmxAgent
```

   On **Mediation Servers**:

```
# pm.set off JmxAgent; pm.set on JmxAgent
# pm.set off dsapi; pm.set on dsapi
# pm.set off DataExport; pm.set on DataExport
```

Configure Production Interface (optional)

In case of acquisition and mediation server a production network may be available, this production network shall be used for the data transfer between the acquisition and mediation servers. The procedure gives step to add the virtual network interface on the acquisition and mediation virtual machines. The production network can be configured using the created interface by following the steps in the CCM user guide [9]

The production interface on the bare-metal server is setup differently than on the virtual machine.

Production Interface on Bare-metal server

In case of bare-metal server the production interface can be eth02 or eth04. These interfaces are already available in the primary NIC card, which is typically two port or four port card. The eth01 is used for the management IP address

on the server, the production network can be either eth02 or eth04. In case there is a need for redundancy for the production network, then bonded interface of eth02 and eth04 can be created. It is recommended to create "bond1" interface in case of redundancy requirement as bond0 is already used on the Integrated acquisition server. The interface(s) used for the production network must be connected to the appropriate switch and the production network must be reachable from all the servers in the sub-system.

Configure Bonded Interface (Optional)

Note: In case of bonding, if any of the interface is down e.g. eth02 or eth04, then no alarm will be raised by the platform or the application.

1. Login into the server's console
2. To create the bonded interface, as root, run:

```
# netAdm add --device=bond1 --bootproto=none --type=Bonding    --onboot=yes --mode=active-backup --miimon=100 --bondInterfaces=eth02,eth04
```

The route can be added from the CCM application when the production interface is configured from the CCM.

Production Interface on virtual machine server

In case of virtual machine server, a new virtual interface needs to be added. The new interface can be added by creating a new bridge on the host machine and during the creation of the guest machine add one more interface in the guset using the newly created production bridge. The bridge on the host machine should use the host interface that is configured with the production network.

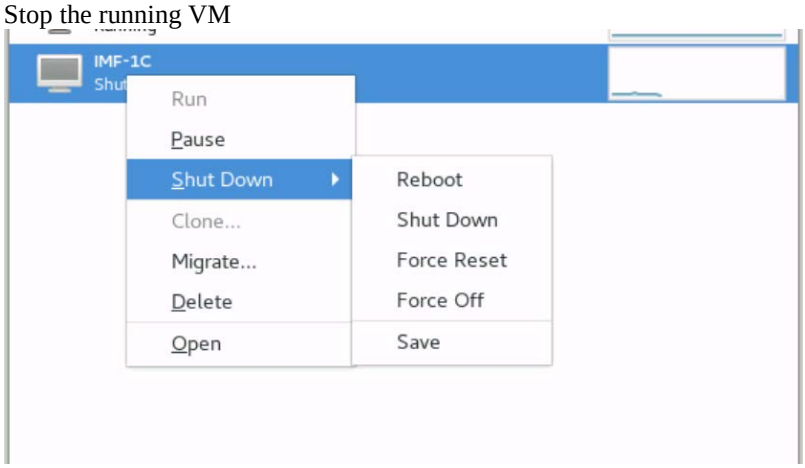
The production bridge can be created by following the procedure defined in Network Bridge Creation in Virtual Machine. In case the acquisition and mediation servers are on the same host then **internal production bridge** needs to be created otherwise if the acquisition and mediation servers are on the different hosts then **external production bridge** needs to be created.

In case the acquisition probed server VM needs to be created then use "Probed Guest Creation"
In case the mediation server VM needs to be created then use "Mediation Guest Creation"

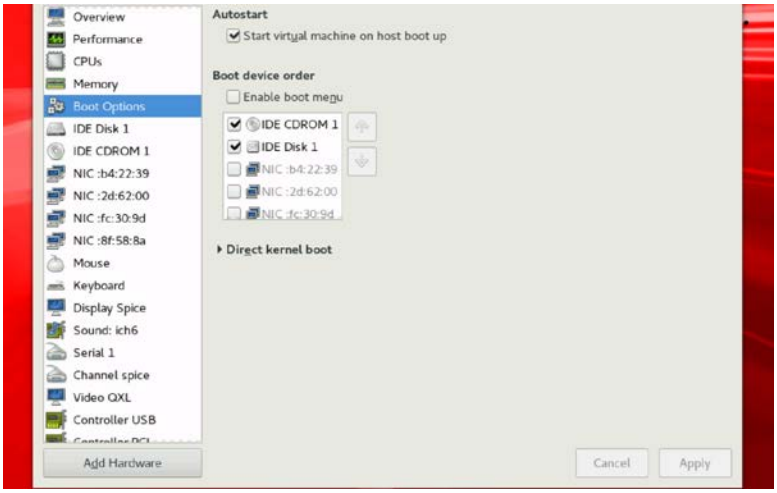
In case of the integrated acquisition server VM creation refer to the Integrated Server Guest Creation and Installation , however the production interface needs to be added separately. This can be done by following the procedure "Adding Production Interface to existing virtual machine"

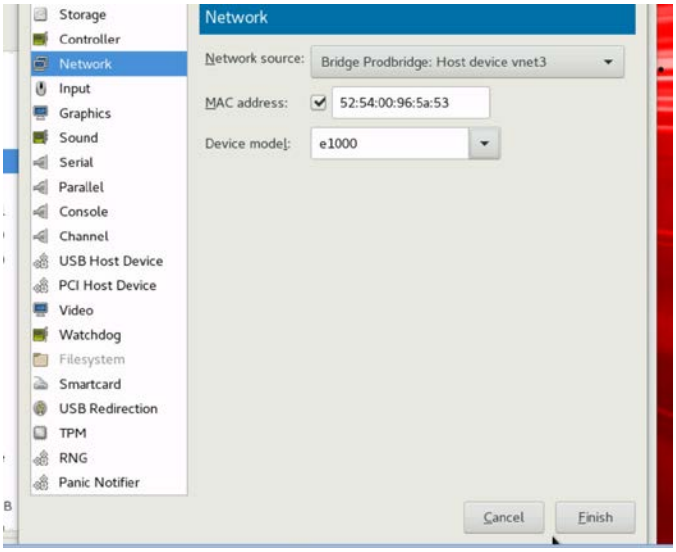
Adding Production Interface to existing virtual machine

1. Stop the running VM

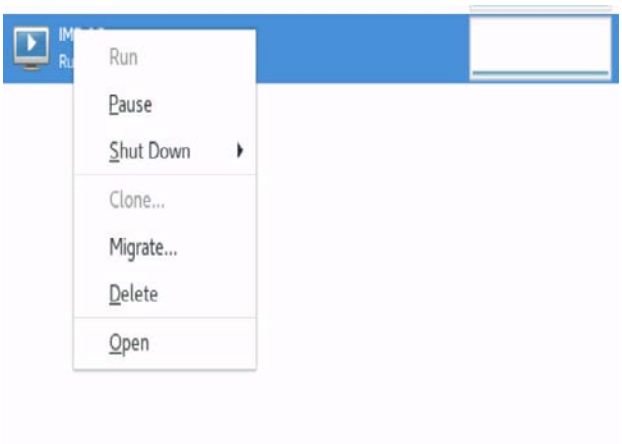


2. Open the properties of the VM
    a. Add a new Hardware
    b. Select the Network Source as “Production Bridge”
    c. Devide Model as “e100”

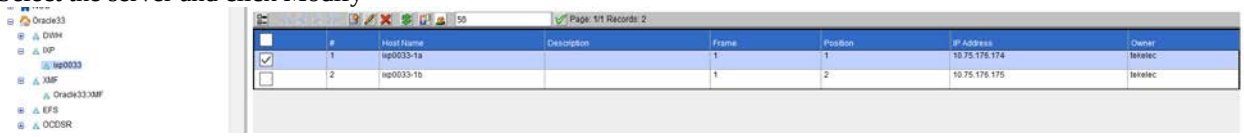




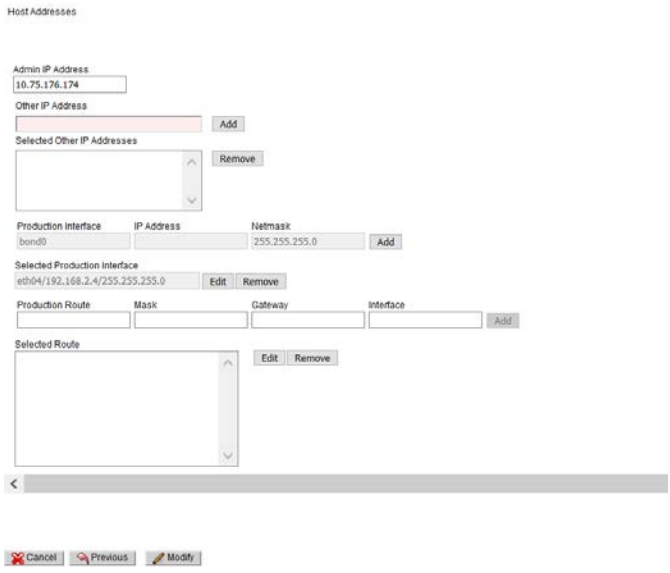
3. Click on Finish and Apply
4. Start the VM, by selecting the “Run”



5. Follow the procedure Server network device configuration to rename the production interface to “eth04” on the acquisition and mediation VMs.
6. Configure the Production Interface on the CCM application, for each server in the sub-system
    a. Login to NSP as “TklcSrv” user
    b. Go to CCM->Equipment Registry->Sites
    c. Select Acquisition or Mediation Site->sub-system
    d. Select the server and click Modify



    e. Navigate to the Production Interface Screen



    f. Add the production interface details, use the interface that was created (based on the bare-metal or virtual production interface configuration)
    g. Click on Modify to complete the action.
    h. Apply the changes.

Note: The above steps should be performed for all the servers in the sub-system.

7. On all the servers in the sub-system, restart the processes, as cfguser:

Before restarting the processes, please check if all the points mentioned in section Important Points for configuring production Interface are taken care of.

On **Acquisition Servers**:

```
# pm.set off pduServer0; pm.set on pduServer0
```

On **Mediation Servers**:

```
# pm.set off IxpForward; pm.set on IxpForward
# pm.set off IxpManage; pm.set on IxpManage
```

Verification

The production interface is configured now and added to the acquisition or mediation server. The data transfer on the DTS protocol now will happen using the production network IP. This can be verified using the netstat command on the acquisition and medition server.

On mediation server:

```
[cfguser@ixp0033-1b ~]$ netstat -anp| grep 2222 | grep -i estab
(Not all processes could be identified, non-owned process info
  will not be shown, you would have to be root to see it all.)
tcp        0      0 192.168.2.5:2222            192.168.2.5:58584           ESTABLISHED 21290/IxpForward
tcp        0      0 192.168.2.5:58552           192.168.2.5:2222            ESTABLISHED 20823/IxpStore
tcp        0      0 192.168.2.5:58568           192.168.2.5:2222            ESTABLISHED 26600/IxpStore
tcp        0      0 192.168.2.5:57252           192.168.2.7:2222            ESTABLISHED 20696/IxpBuild
tcp        0      0 192.168.2.5:33672           192.168.2.4:2222            ESTABLISHED 19956/IxpOperate
tcp        0      0 192.168.2.5:33834           192.168.2.4:2222            ESTABLISHED 18643/IxpStore
tcp        0      0 192.168.2.5:2222            192.168.2.5:58532           ESTABLISHED 21290/IxpForward
```

Note: If some connections between IxpForward and IxpStore/IxpOperate still show management interface even after configuration of production interface then check if the IxpStore/IxpOperate processes are receiving any data on the corresponding streams, in case there is no data on the corresponding streams then management interface is used and as soon as data starts coming on the streams the connection will be switched to the production network IP address.

On Acquisition server:

```
[cfguser@pmf0033-0a ~]$ netstat -anp| grep 2222
(Not all processes could be identified, non-owned process info
  will not be shown, you would have to be root to see it all.)
tcp        0      0 :::2222                     :::*                        LISTEN      5440/pduServer
tcp        0      0 ::ffff:192.168.2.7:2222     ::ffff:192.168.2.5:57252    ESTABLISHED 5440/pduServer
tcp        0      0 ::ffff:192.168.2.7:2222     ::ffff:192.168.2.4:56892    ESTABLISHED 5440/pduServer
tcp        0      0 ::ffff:192.168.2.7:2222     ::ffff:192.168.2.4:56890    ESTABLISHED 5440/pduServer
tcp        0      0 ::ffff:192.168.2.7:2222     ::ffff:192.168.2.4:56904    ESTABLISHED 5440/pduServer
tcp        0      0 ::ffff:192.168.2.7:2222     ::ffff:192.168.2.4:56888    ESTABLISHED 5440/pduServer
tcp        0      0 ::ffff:192.168.2.7:2222     ::ffff:192.168.2.5:57270    ESTABLISHED 5440/pduServer
tcp        0      0 ::ffff:192.168.2.7:2222     ::ffff:192.168.2.5:57326    ESTABLISHED 5440/pduServer
```

Important Points for configuring production Interface

1. The production network interface name can only be “eth01 to eth09” or “bond0 to bond9”. On Integrated acquisition server, the eth01 and eth03 are used for the yellow and blue VLAN, so eth01 and eth03 can’t not be used. The management interface is always used as eth01, so eth01 should never be used for the production interface name on the CCM application.
2. **By default** the production interface name on the acquisition server is set to “bond1”, however it should be set to the same name as configured from CCM application. This can be done by the following steps:
    a. As cfguser on the ActMaster server, ivi StringParam
    b. Update the parameter “ProductionInterface” with appropriate value, e.g. “eth04”

Yes|ProductionInterface|eth04|Production Network Interface, **default value=bond1**, modify it to the configured value

c. Save the file

d. Apply Y
APPLY THE CHANGES [yn]?y

3. In case the production network is setup for the acquisition server(s) then all the mediation servers in all the mediation sub-system must also be setup with the production network. The DTS communication will only happen either between production network or management network, if no production network is setup then DTS communication will happen using the management network, however, if the production network is setup, then it must be setup for all the acquisition and mediation sub-system.
4. In case of DTS connection, the first connection is always made using the management network and if the production interface is configured and connected on the acquisition server, then connection is switched to the production interface and data transfer happen on the production interface.
5. On mediation server, if there is no data coming on the stream then in the **netstat** the connection will show the management IP address as indicated below. This will be switched to the production IP as soon as data starts coming in.

```
tcp        0      0 10.75.176.175:41602     10.75.176.175:2222      ESTABLISHED
26603/IxpStore
tcp        0      0 10.75.176.175:2222      10.75.176.175:41602     ESTABLISHED
26603/IxpForward
```

6. On mediation server, there maybe many TIME_WAIT connections in netstat, because of the point 5, so the care must be taken that data should always come on all the streams always, else all such processes where the data is not coming should be turned off.

Appendix D: System Partitioning Recommendation

Applies To :

Oracle Communications Performance Intelligence Center (PIC) Software - Version 10.4.0 [Release 10.0]
Information in this chapter applies to any hardware platform.

Purpose

Provide a guidance for the system partitioning when installing Oracle Linux.

Management

Mount point	Size
/	50GB
/boot	500MB
/home	100GB
swap	size of the RAM (64GB or 128GB)
/usr	100GB
/opt/nsp	100GB
/opt/oracle11 or /u01/app	150GB

Mount point	Size
/var/ORCL	Remaining Space (400GB or 700GB)

Data Record Storage

Mount point	Size
/	50GB
/boot	500MB
/home	100GB
swap	size of the RAM (64GB or 128GB)
/usr	100GB
/opt/oracle11 or /u01/app	150GB
/var/ORCL	Remaining Space (500GB or 800GB)

Packet Data Unit Storage

Mount point	Size
/	100GB
/boot	500MB
/home	100GB
swap	size of the RAM (64GB or 128GB)
/usr	Remaining Space (700GB or 1TB)

Prepackage Hypervisor

Mount point	Size
/	5GB
/boot	500MB
/home	5GB
swap	64GB
/var	Remaining Space (1TB)

Prepackage Management

Mount point	Size
/	10GB
/boot	500MB
/home	20GB
swap	32GB
/usr	10GB
/opt/nsp	40GB
/opt/oracle11 or /u01/app	25GB
/var/ORCL	10GB