Oracle® Communications Performance Intelligence Center

Installation Guide

Release 10.2.1

E77485-01

June 2017

ORACLE®

Oracle® Communications Performance Intelligence Center Installation Guide, Release 10.2.1

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

Table of Contents

List of Figures

List of Tables

Chapter 1: About This Help Text

Scope And Audience

This document describes the procedures to install a "Oracle Communications Performance Intelligence Center" system at Release 10.2.1.

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 Security Guide of Performance Intelligence Center.

Requirements and Prerequisites

Hardware Requirements

Please refer to Hardware Guidelines. of Performance Intelligence Center.

Software Requirements

The following software is required for the release 10.2 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
- Acquistion Server
- Acquisition datafeed
- TPD

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

https://edelivery.oracle.com/

Please refer to KM notes which are constantly updated with last improvements :

Title	MOS
Oracle Linux on Third-Party Server Installation Guide for Performance Intelligence Center Products	KM_2061666.1
Oracle 12c ASM and Database on Third-Party Server Installation Guide for Performance Intelligence Center Products	KM_2151499.1
Upgrade Oracle Communications Performance Intelligence Center, is providing some guidances	KM_1984685.2
Performance Intelligence Center **Data WareHouse Server (DWS)** on Third-Party Server Installation Guide	KM_2028670.1
Performance Intelligence Center **Packet Data Unit Storage (PDU)** on Third-Party Server Installation Guide	KM_2034894.1
Management Server (NSP) on Third-Party Server Installation Guide for Performance Intelligence Center Products	KM_2164544.1
Management Server (NSP) on TPD system Installation Guide for Performance Intelligence Center Products	KM_2251899.1
Installation & Configuration for Oracle Java SE	KM_1412103.2
Capacity management good practices	KM_1683859.2
How to Configure NTP	KM_2083591.1

Reference Documents

[1] Platform Configuration Guide, Tekelec Platform release 7.4

[2] TPD Initial Product Manufacture, Tekelec Platform release 7.4

[3] HP Solutions Firmware Upgrade Pack 2.2.10, Tekelec Platform release 7.4

[4] Oracle Firmware Upgrade Pack, Tekelec Platform release 7.4

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

[6] Hardware Guidelines, Performance Intelligence Center release 10.2.1

[7] Security Guide, Performance Intelligence Center release 10.2.1

[8] Quick Start Guide, Performance Intelligence Center release 10.2.1

[9] Centralized Configuration Manager Administrator Guide, Performance Intelligence Center release 10.2.1

Performance Intelligence Center release 10.2.1 is using Comcol 7.3 with TPD 7.4

Chapter 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 7.1 based server and can be shared with a Data Record Storage and/or a PDU Storage.
   - Can be deployed on TPD 7.4 only when already installed in a previous release of PIC on TPD.
2) **Data Record Storage:**
   - Can be deployed on Oracle Linux 7.1 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 7.1 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 refenced 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.
   - 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.

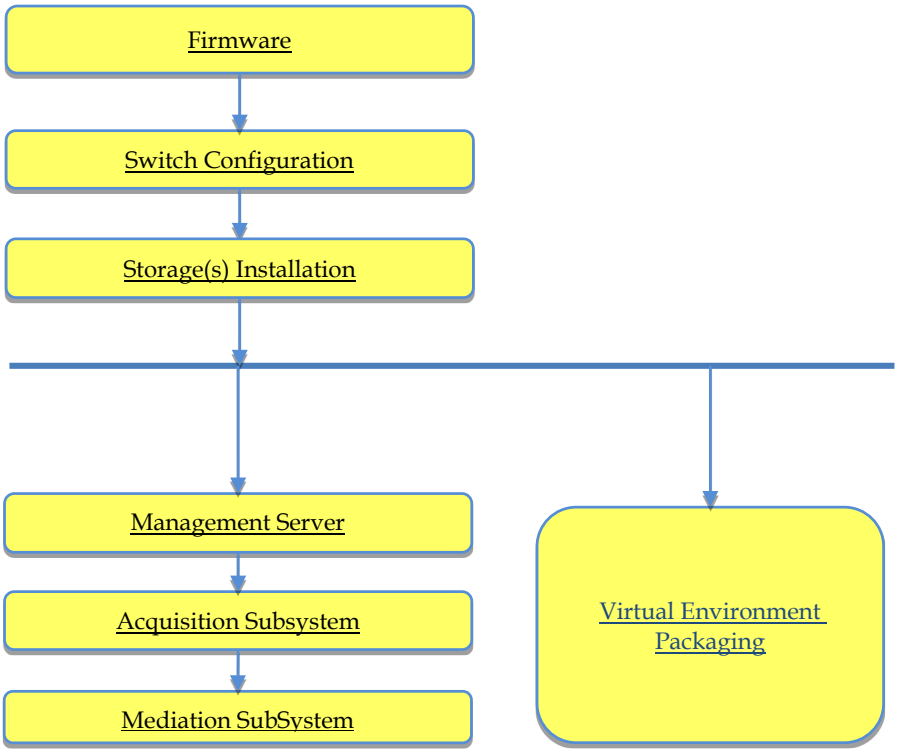
High Level Manufacturing

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 KM_2061666.1 during the Oracle Linux installation on RMS server.

Apply the last firmware upgrade, Tekelec Platform release 7.3:

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 to KM_2028670.1 for **Data WareHouse Server (DWS)** Installation on RMS server.

PDU Storage(s) Installation

Refer to KM_2034894.1 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 KM_2061666.1 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 6: Virtual Customized Package
2. Chapter 7: Prepackaged DSR Monitoring

Management Server

Please refer to KM_2164544.1 for **Management Server (NSP)** Installation.

For existing Management Server already installed in a previous release on top of TPD, please refer to KM_2251899.1

The next chapters are describing the post installation.

Change Customer Icon (Optional)

Execute the procedure Change Customer Icon (Optional)

Install Optional Applications

Execute the procedure Install Optional Applications

Configure Purchased Tokens

Execute the procedure Configure Purchased Tokens

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
```

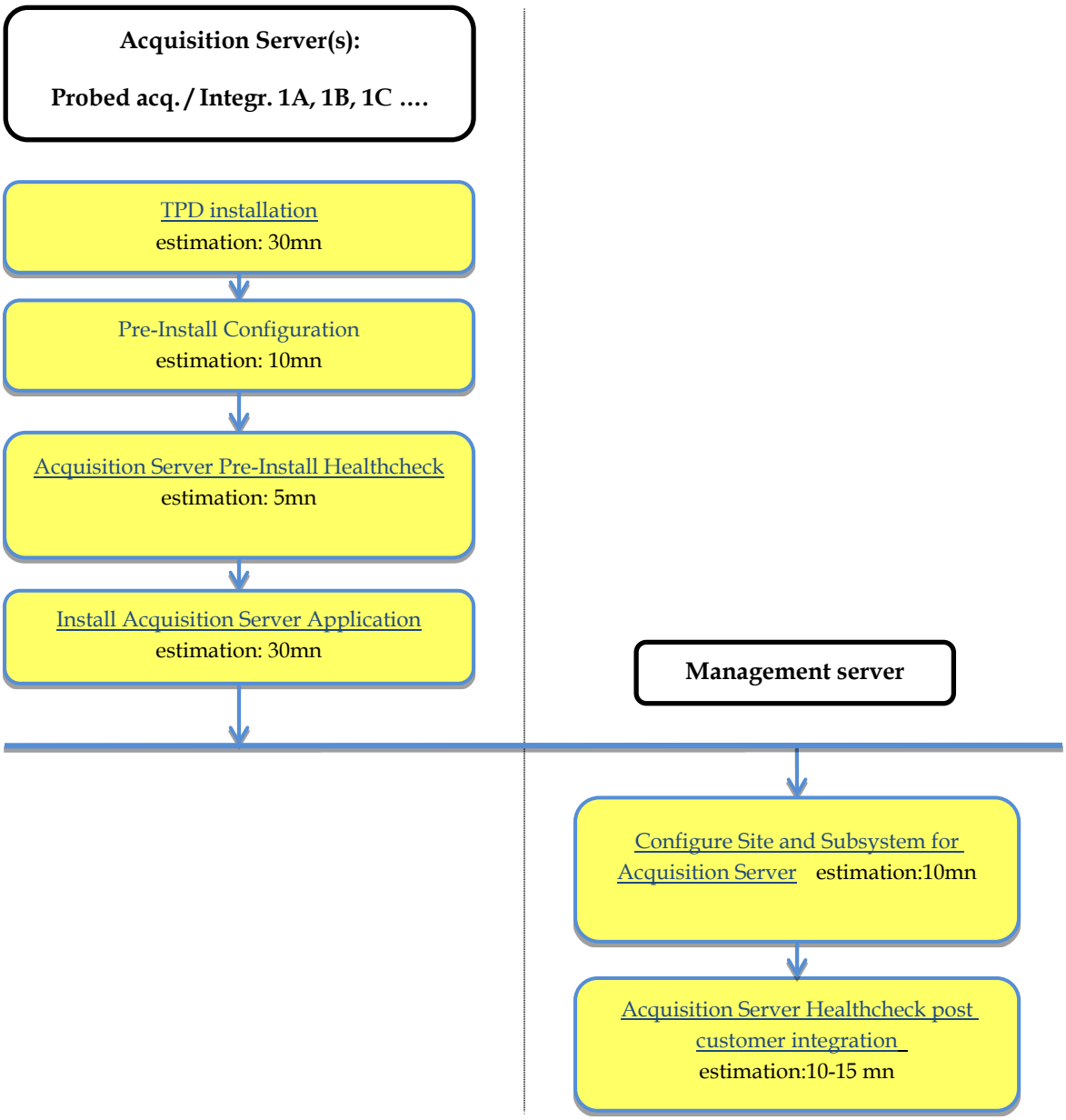
If the result of above command still contains DBA role in result set then refer to Appendix D: My Oracle Support

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.

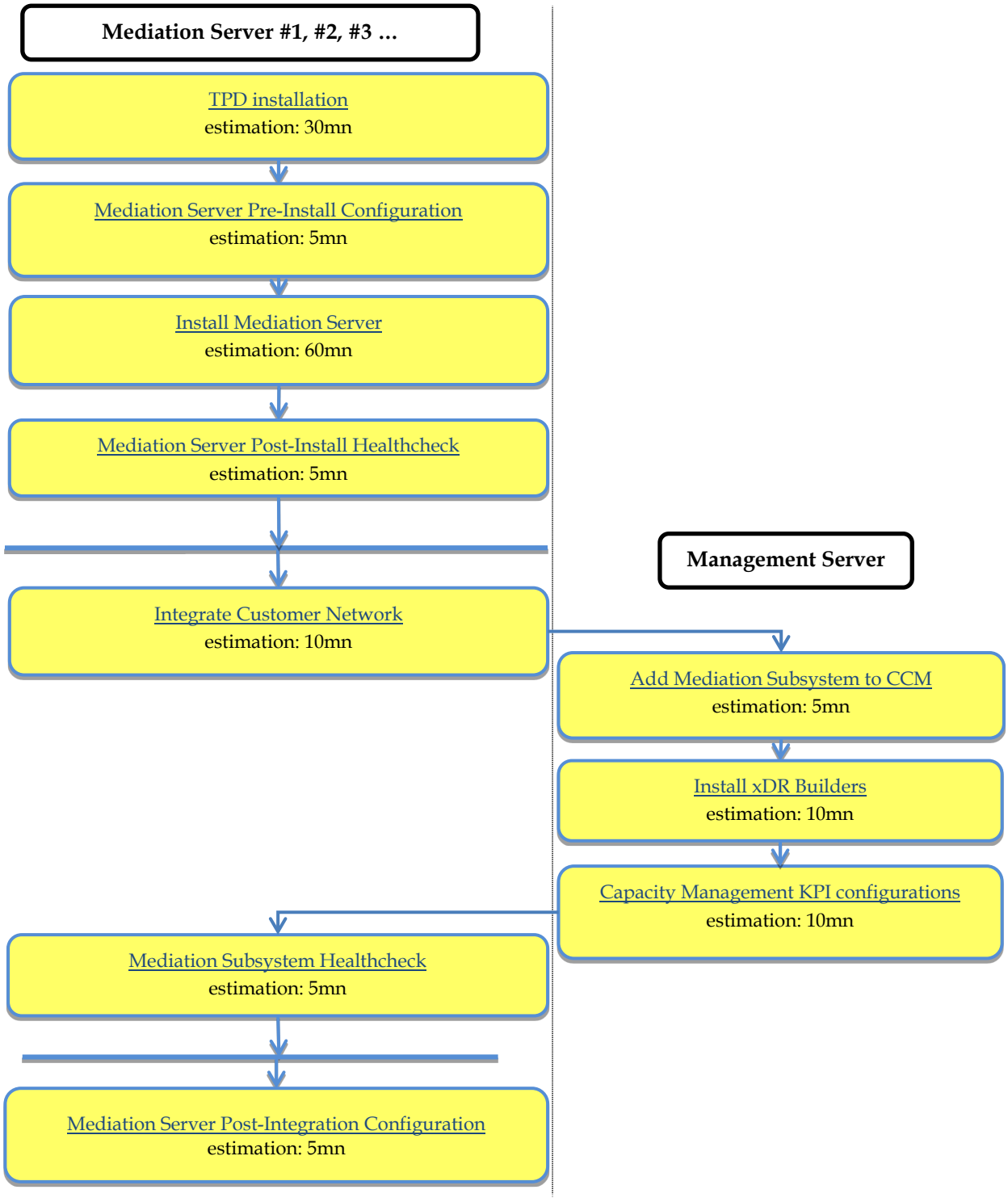
Figure 2. Integrated and Probed Acquisition SubSystem Installation



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



Chapter 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

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

Supported TPD Hardware	Recommended Command	Comments
HP RMS G6, Gen8, Gen9	TPDnoraid console=tty0	
X5_2, X6_2	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. **Note**: If the error message "*The IPM FAILED on this server. Run verifyIPM for details*" shows up on the console, until the bug 24841996 (and the related bug 24842022) is fixed, it is required to IPM the server again with the command **TPDlvm** (without **scrub**).

Table 1: TPD and HW supported for Performance Intelligence Center 10.2.1

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

Chapter 4: 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 assigment 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 Integarted 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 informationon 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 D: 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: 7.0.3.0.0-86.40.0
04:57:31: XMF VERSION: [ 10.2.0.0.0-24.1.0 ]
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
```

4. Modifying IP header format version on Probed Acquisition Server:

   This procedure describes how to modify the IP Header format version for IP Raw PDUs on Probe. By default, the version support is 0 in LongParam table. This is done to support the use case when xDR builders are still using the old IP header format, However on fresh installed site this parameter must be changed to indicate new version on Probe Server. The current version supported for 10.2 is "2".

   This support is activated by the parameter **'IPHeaderFormat'** inside the '**LongParam**' table:

   ```
   Yes|IPHeaderFormat|2|Ip Header version (2 -V2, 1 -V1, 0 -V0: Default-0)
   ```

   The parameter can be modified using the following command:

   ```
   $ iset -fvalue=2 LongParam where "name='IPHeaderFormat'"
     === changed 1 records ===
   ```

   After modification of this parameter, the **pduServer0 process** must be restarted using

   ```
   $ pm.set off pduServer0
   $ pm.set on pduServer0
   ```

   Note: A clobber on the Probe Acquisition server will reset to the default value.

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

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

Chapter 5: 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 8.1.2 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 D: 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: 7.0.1.0.0-86.20.0
08:44:00: IXP VERSION: [ 10.1.5.0.0-3.2.0 ]
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 D: 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 D: 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. Please 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, 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 D: 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 D: 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. CapacityManagement 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 Capacity management good practices on My Oracle Support

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* please 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 an 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 an 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.

Chapter 6: 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 cannot be virtualized. It is possible to use E5-APP-B card in the EAGLE for the integrated acquisition when the traffic figures are compatible with this choice.

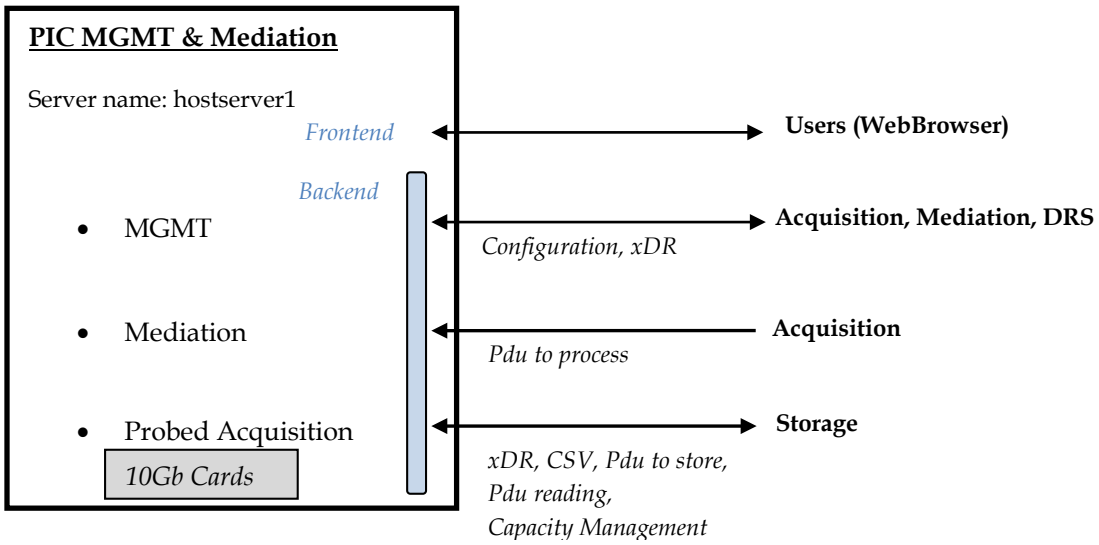
Support:

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 components for the virtualization on the same server are:

- 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:



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, please refer to the chapter **Prepackaged DSR Monitoring**.

Chapter 7: Prepackaged DSR Monitoring

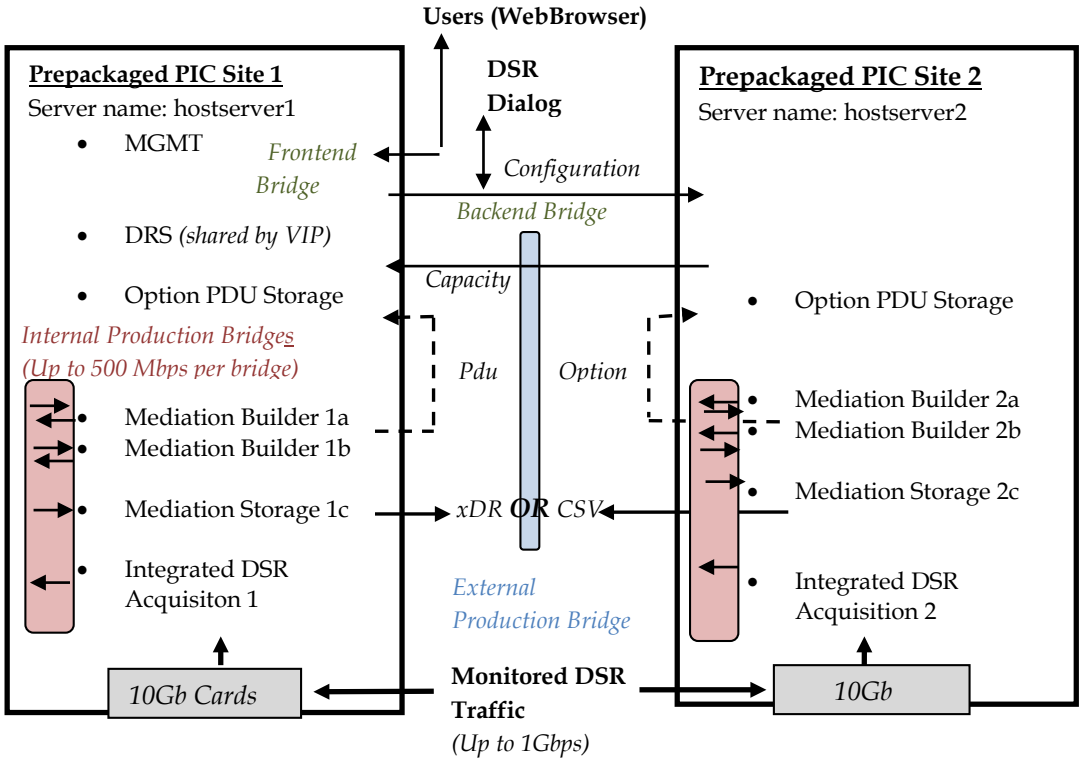
Configuration Overview

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 Reference Documents).

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 3: Resources Performance Intelligence Center Virtual Machine for DSR Monitoring

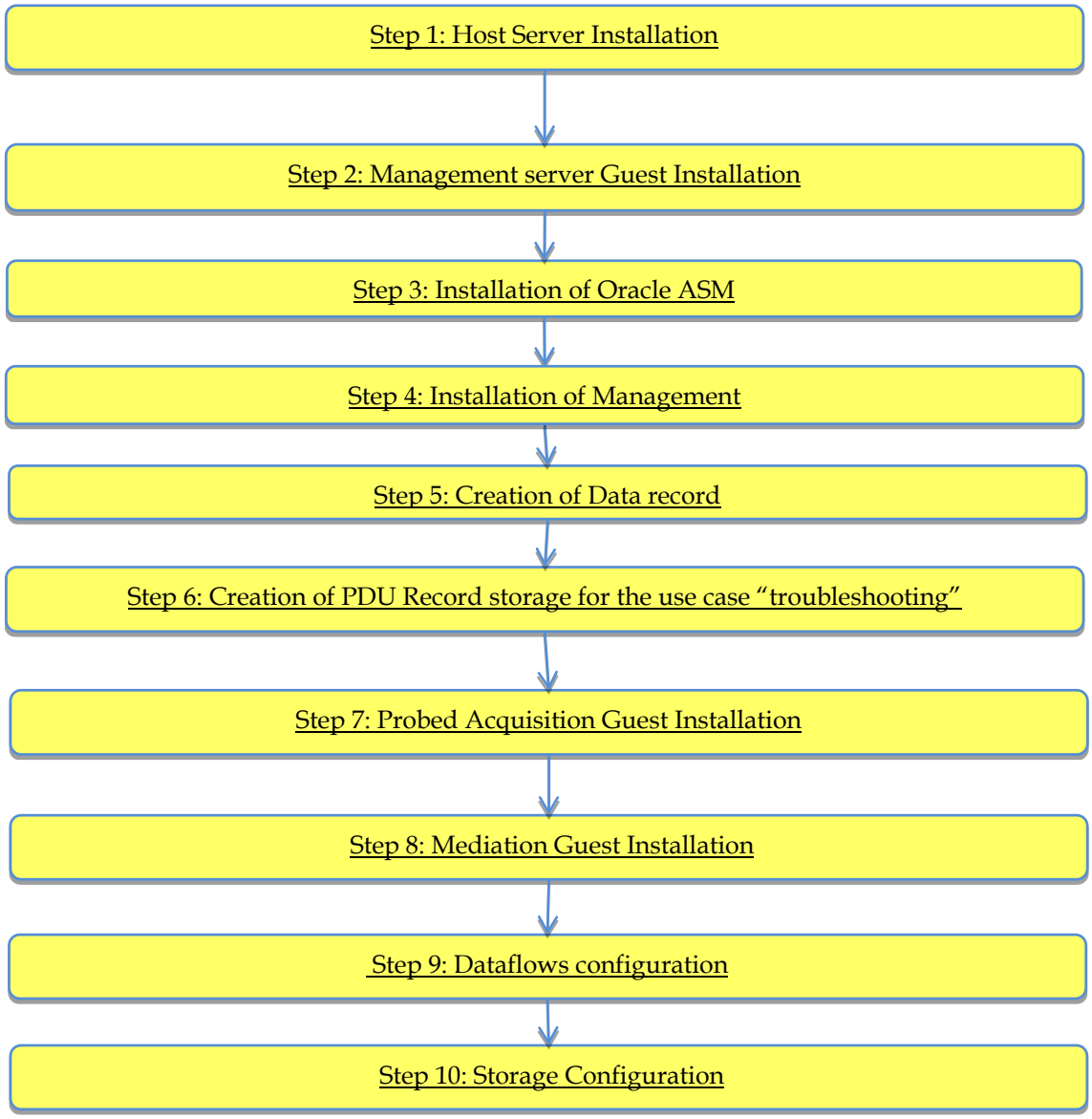
Configuration Steps

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 document Oracle linux on Third-Party Server Installation KM_2061666.1

   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 KM_2174665.1

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

(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 10Gb Ethernet links are to be directly handled by a Probed Acquisition guest. Execute the following procedure to enable the PCI pass through mode:

   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 10Gb 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
```

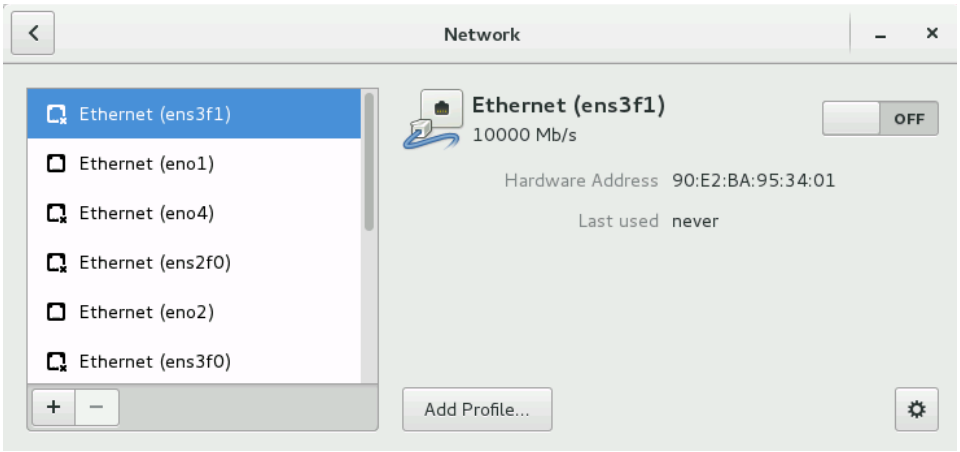
d. repeat both previous steps to detach the remaining devices

(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 KM_2061666.1

   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 KM_2174665.1

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 KM_2061666.1

   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 KM_2174665.1

   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 document Oracle ASM and database on Third-Party Server Installation KM_2062491.1

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 the document Management Server on Third-Party Server Installation KM_2164544.1.

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 document Data WhareHouse Server (DWS) on Third-Party Server Installation KM_2028670.1 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
    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 document Packet Data Unit Storage on Third-Party Server Installation KM_2034894.1

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-7.0.3.0.0_86.40.0-OracleLinux6.7-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-7.0.3.0.0_86.40.0-OracleLinux6.7-x86_64.iso hdb --type
cdrom --mode readonly
# virsh reboot VM_PMF_0a
```

3. In the guest's console, 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
```

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-7.0.3.0.0_86.40.0-OracleLinux6.7-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-7.0.3.0.0_86.40.0-OracleLinux6.7-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-7.0.3.0.0_86.40.0-OracleLinux6.7-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-7.0.3.0.0_86.40.0-OracleLinux6.7-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.

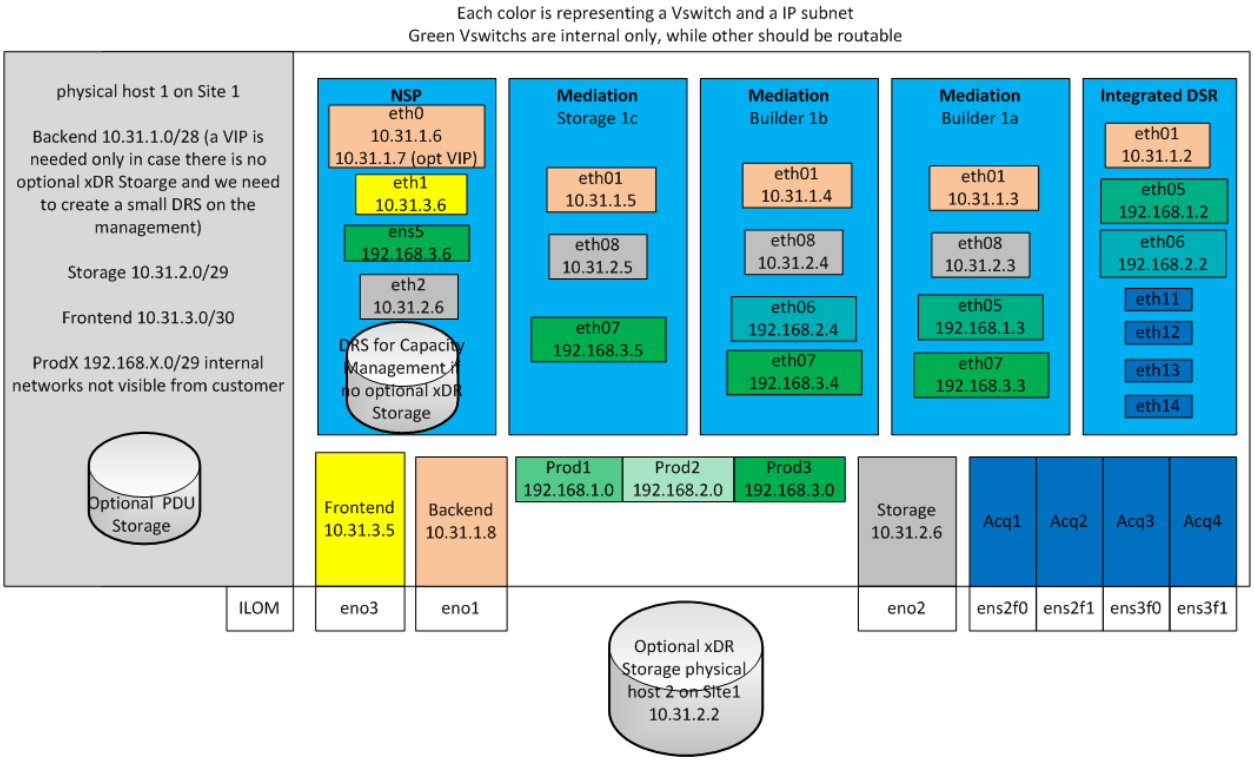
1. Use Case "Accounting"
   a. Activate the CSV option on Management Server
   b. Create the 12 Storages DFP by selecting the "Storage Type" = CSV Files
2. Use Case "Troubleshooting"

   Create the 12 Storages DFP by selecting the "Storage Type" = Datawarehouse

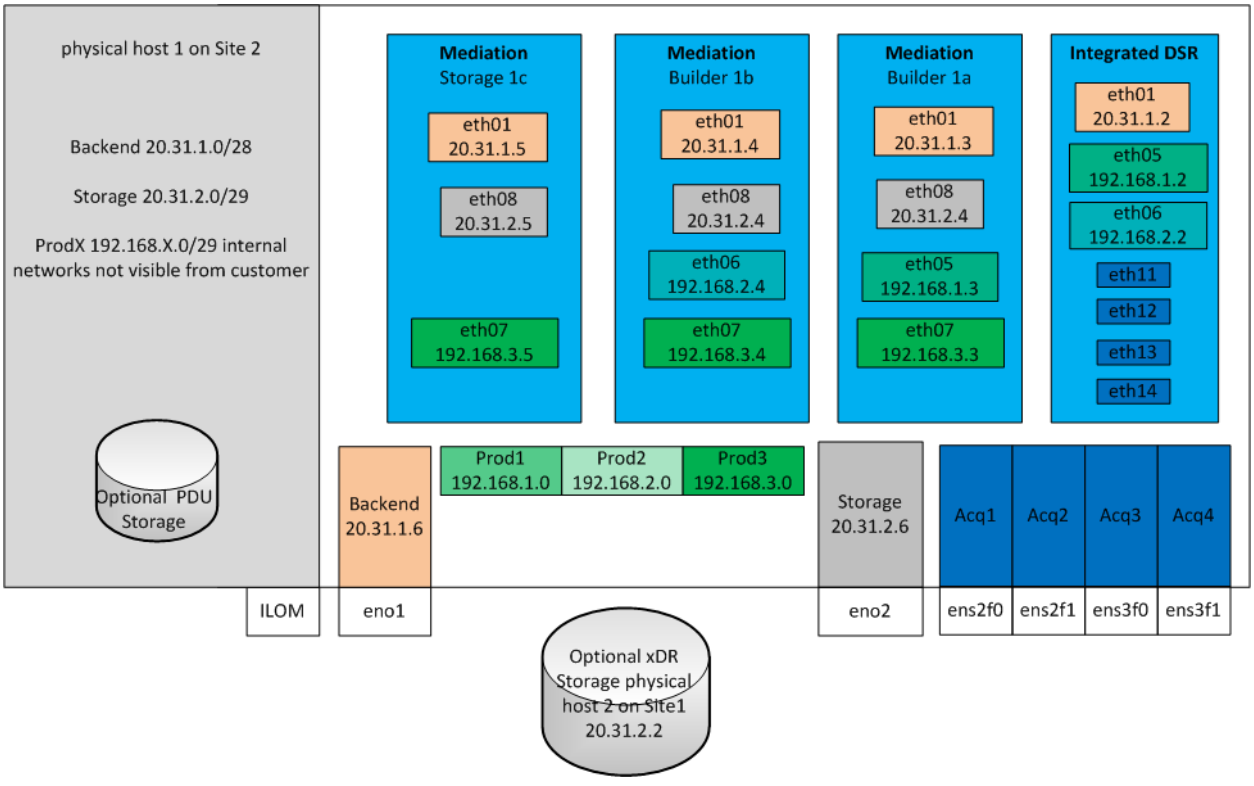
Detailed Schema

Here is a detailed representation of the prepackaged DSR Monitoring.

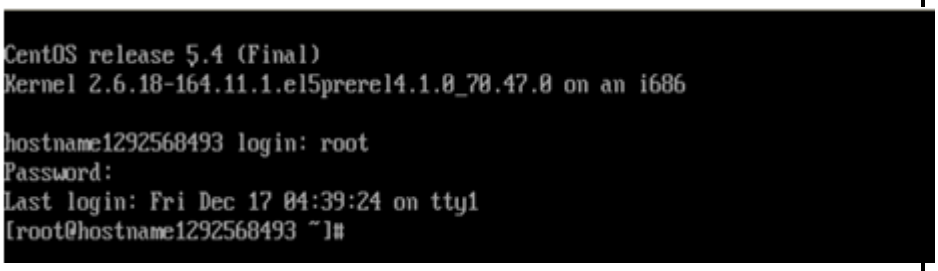
Site 1


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

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

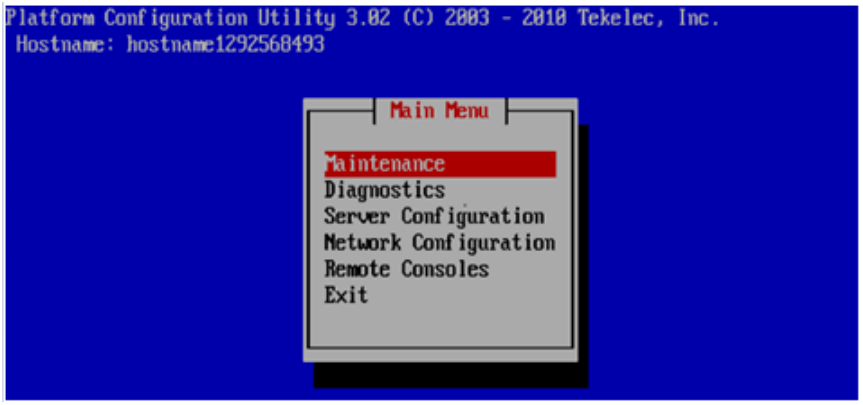
2	Set the IP address and Netmask identified for the eth01 interface	**Command:**
		`# ifconfig eth01 <cust_IP_address> netmask <mask>`
		`#`
		Expected Result:
		No error after executing the command

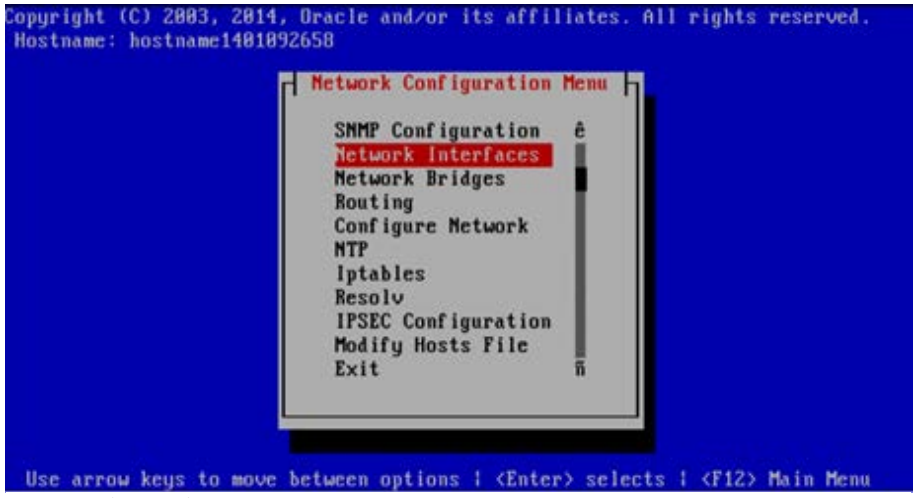
3	Set the default Route Gateway IP address for the eth01 interface	**Command:**
		`# route add default gw <default_route_IP_address>`
		`#`
		Expected Result:
		No error after executing the command

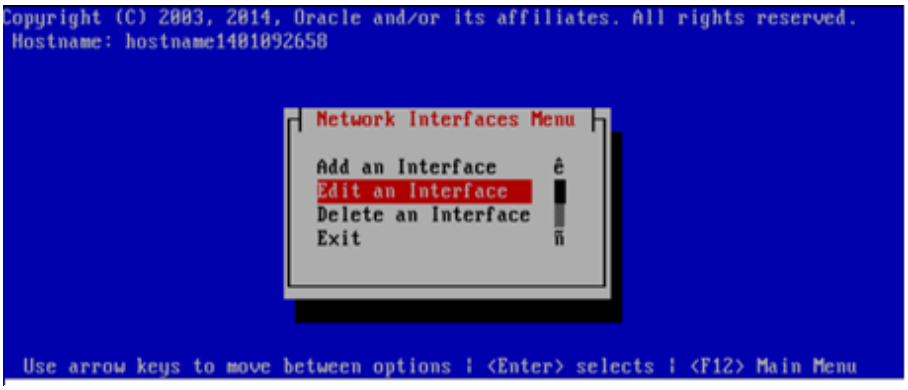
4	Configure remaining servers in frame	**Repeat Steps 1 through 3 for each equipped HP server.**

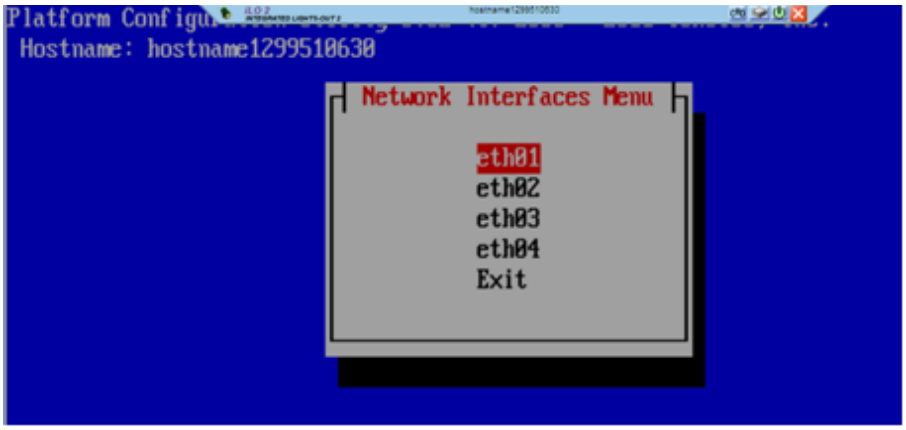
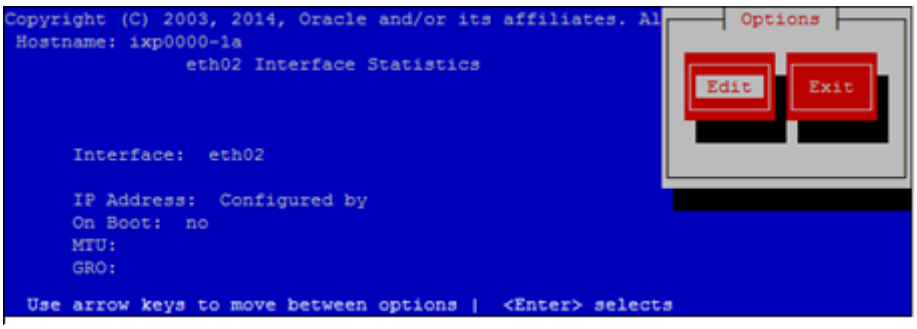
Using platcfg menu procedure

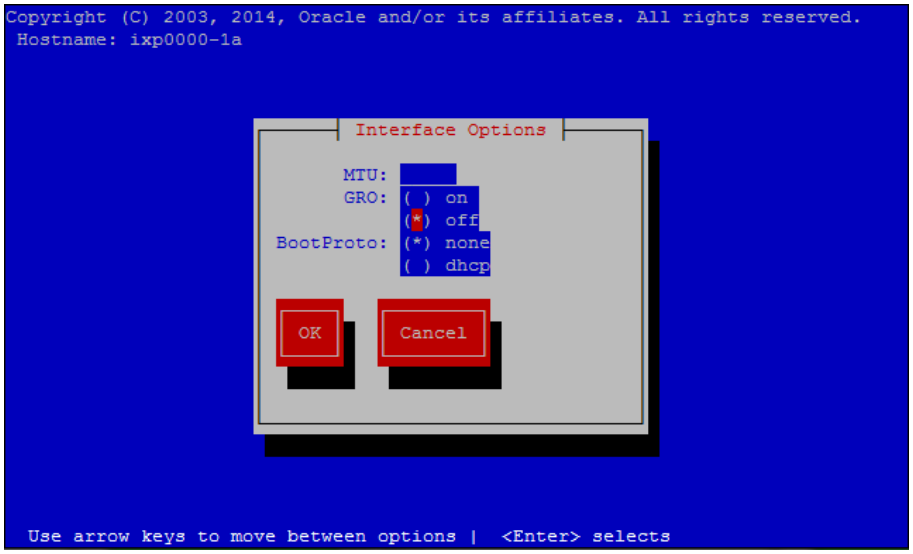
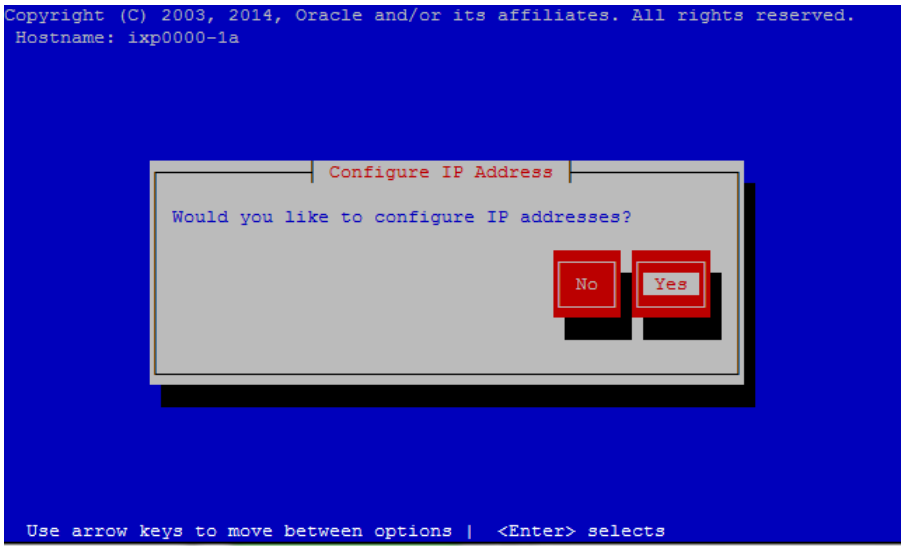
If you configures IP using the command line following the previous procedure, you can skip this procedure is alredy completed

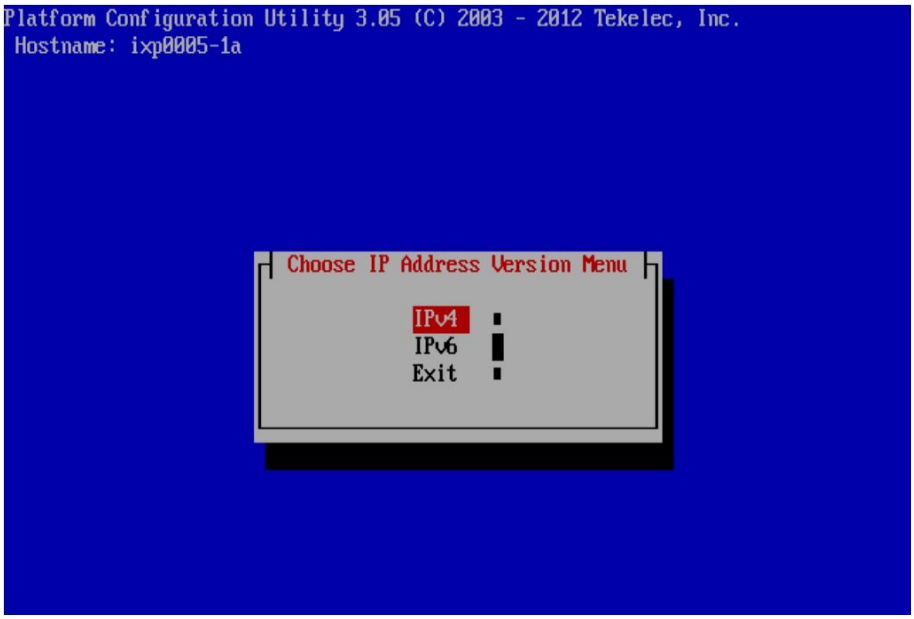
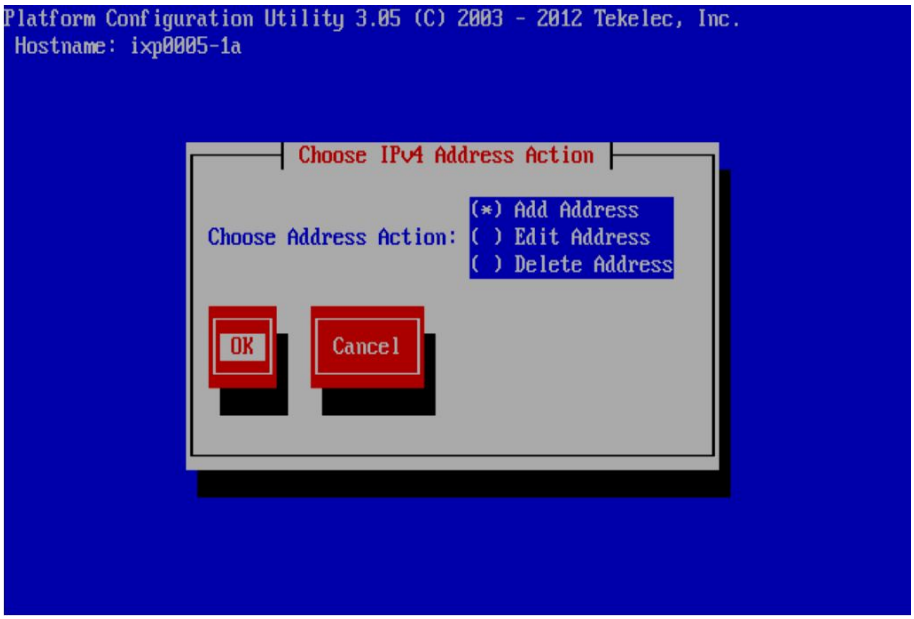
2	Enter the Platform Configuration Utility	To enter the Platform Configuration Utility menu enter: **su – platcfg** 
3	Enter the Platform Configuration Utility	 **Expected Result:** Main Menu of Platform Configuration Utility is displayed

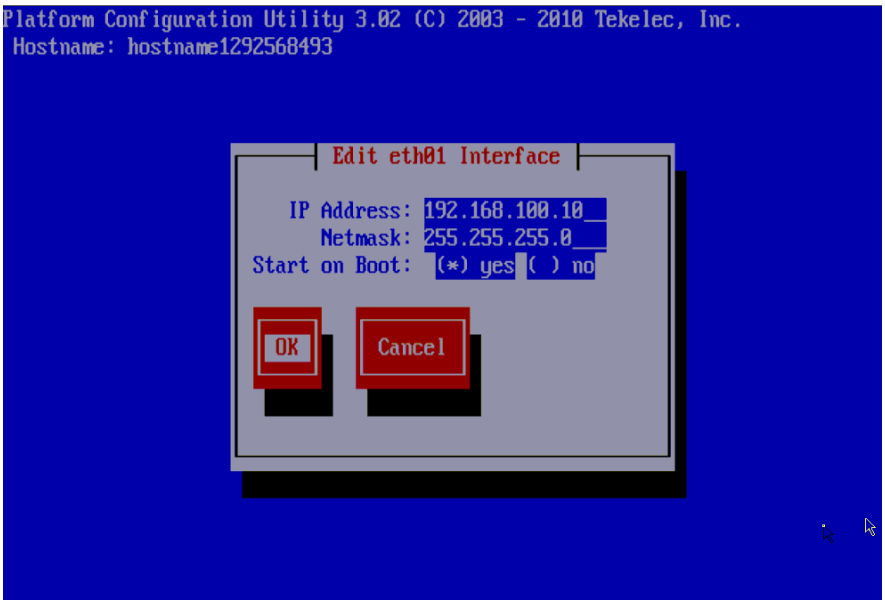
4	Enter the Network Configuration menu of the Platform Configuration Utility	Use the arrow keys on the keyboard to select **Network Configuration** and press [ENTER] to select it.  **Expected Result:** The Network Configuration menu is displayed
5	Enter the Network Interfaces menu	Use the arrow keys on the keyboard to select **Network Interfaces** and press **[ENTER]** to select it.  **Expected Result:** The Network Interfaces menu is displayed

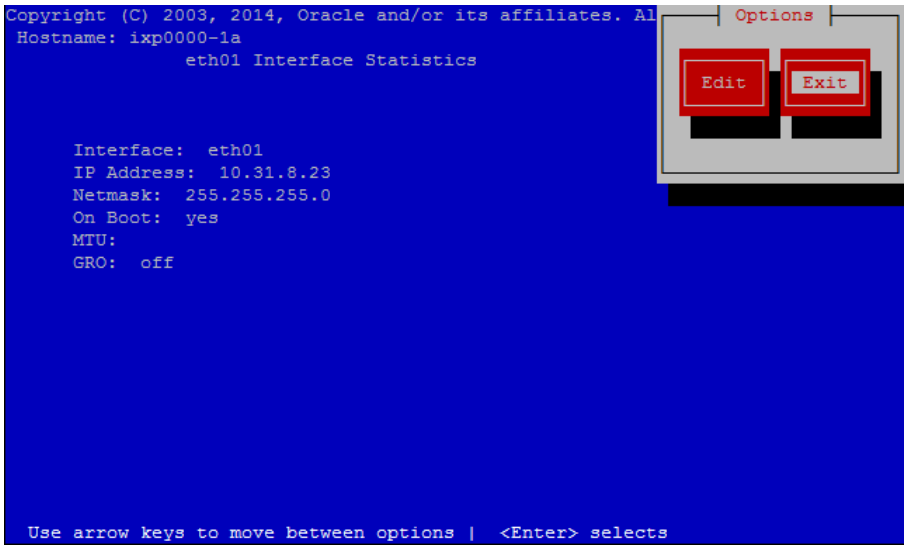
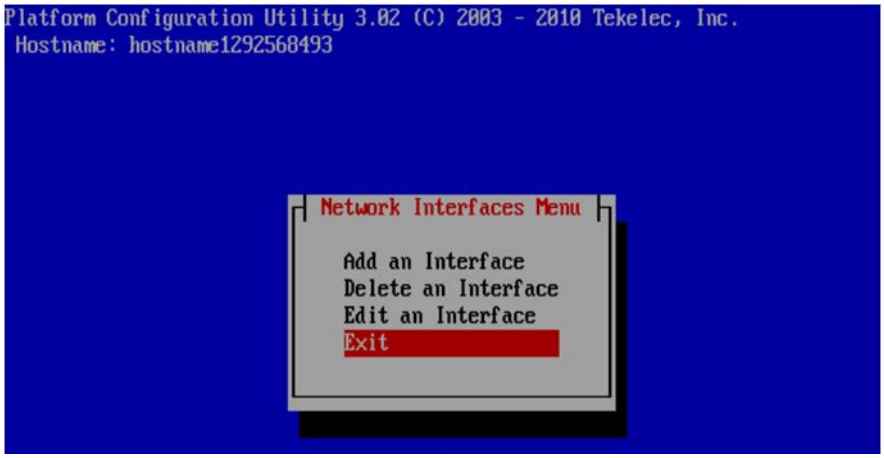
6	Enter the Edit an Interface menu	Use the arrow keys on the keyboard to select **Edit an Interface** and press **[ENTER]** to select it.  **Expected Result:** The Network Interfaces menu is displayed with interface choices eth01 and eth02

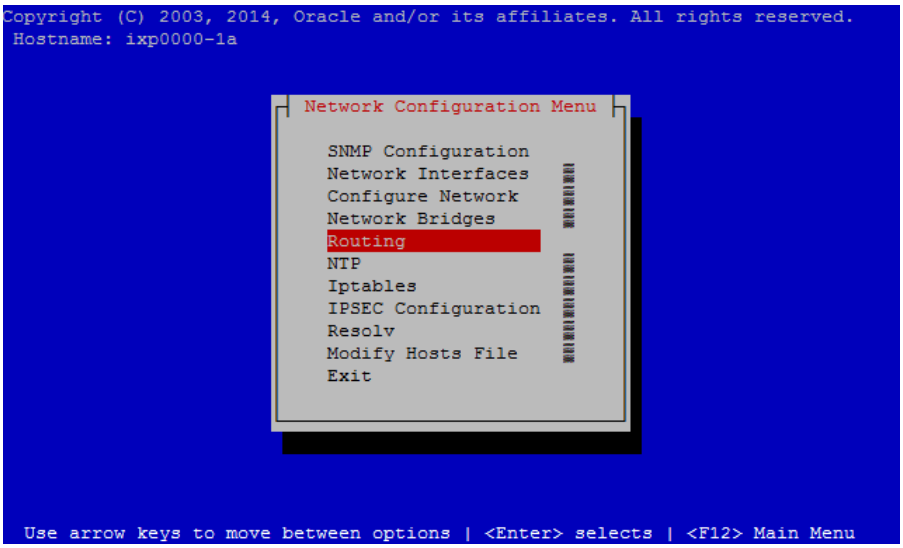
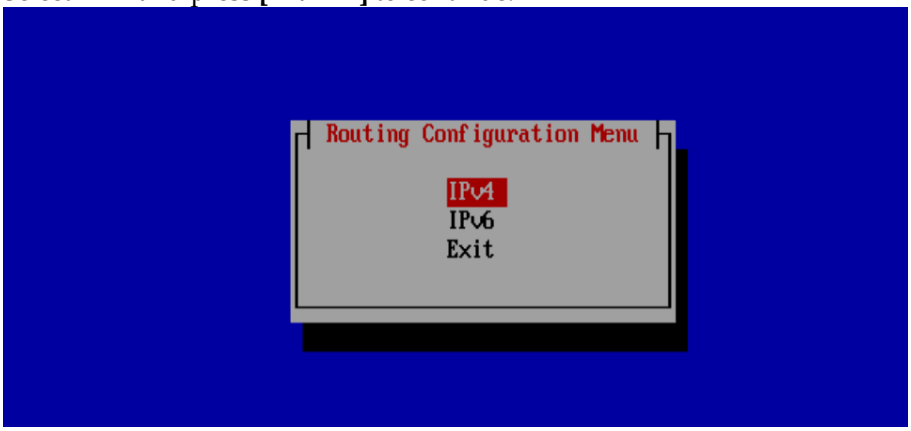
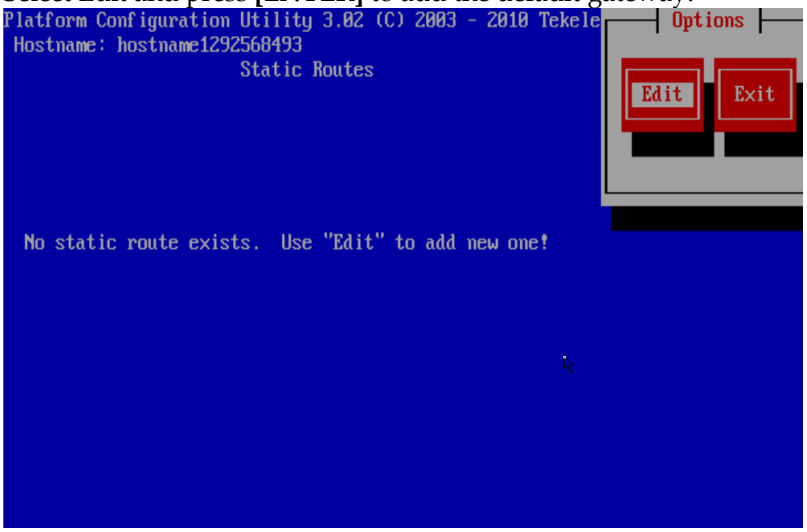
7	Edit the eth01 interface properties	Use the arrow keys on the keyboard to select **eth01** and press **[ENTER]** to select it.  **Expected Result:** The eth01 interface is selected and you are presented with **eth01 Interface Statistics**.  Press the **[ENTER]** key to Edit the properties of eth01. **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.

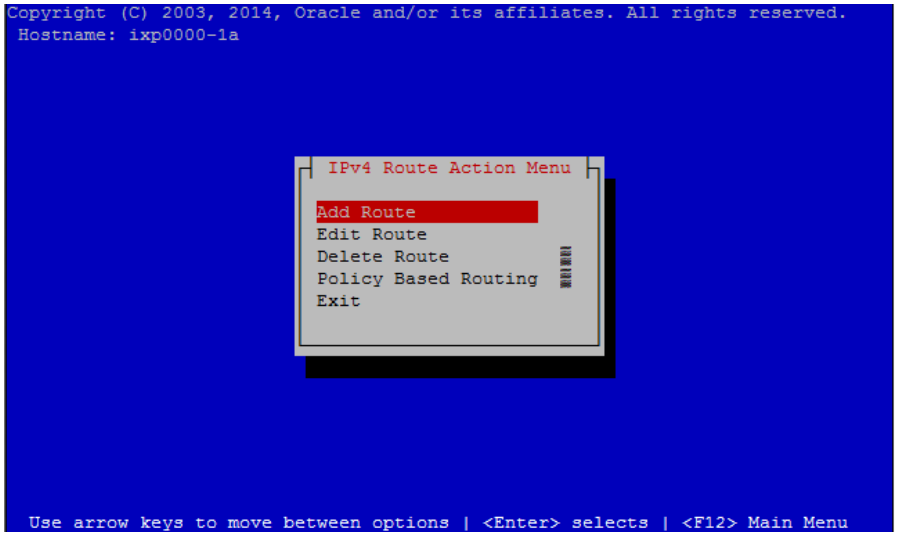
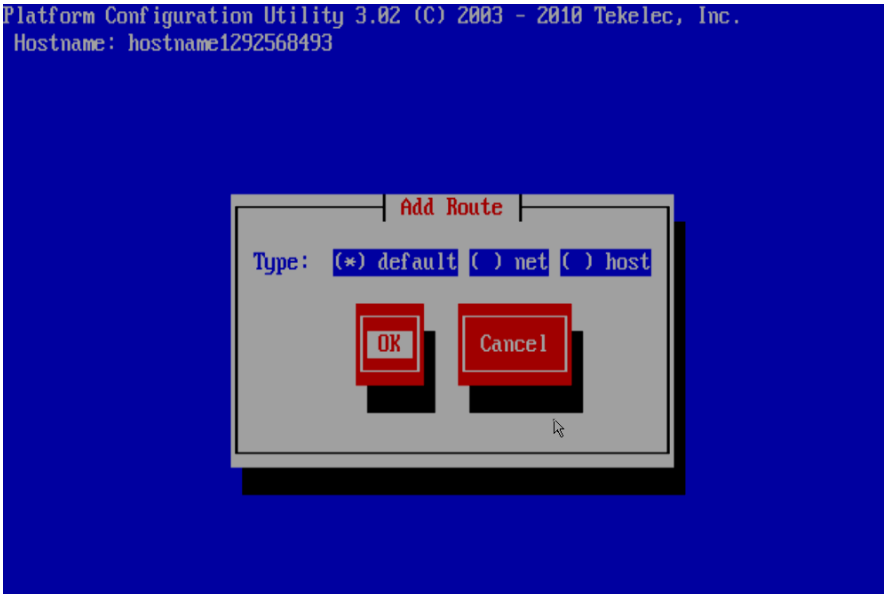
8	Configure MTU, GRO, and boot protocol	Press **[TAB]** to move to off for GRO, then press the **[SPACEBAR]** key to select it. An asterisk will appear once selected. Press **[TAB]** to move to OK, then press the **[ENTER]** key to continue.  **Expected Result:** GRO is set to off and you now see the 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. 

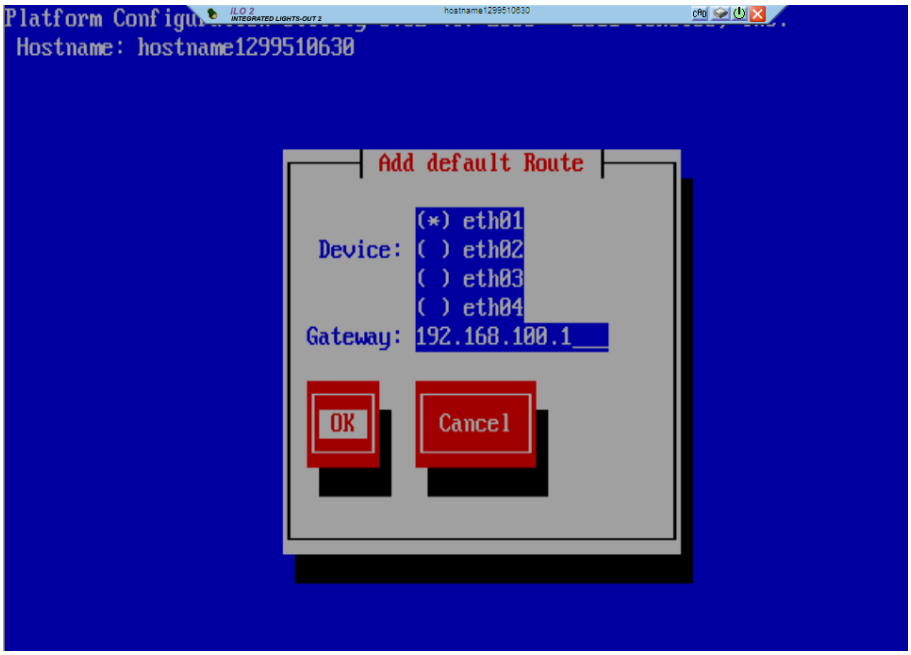
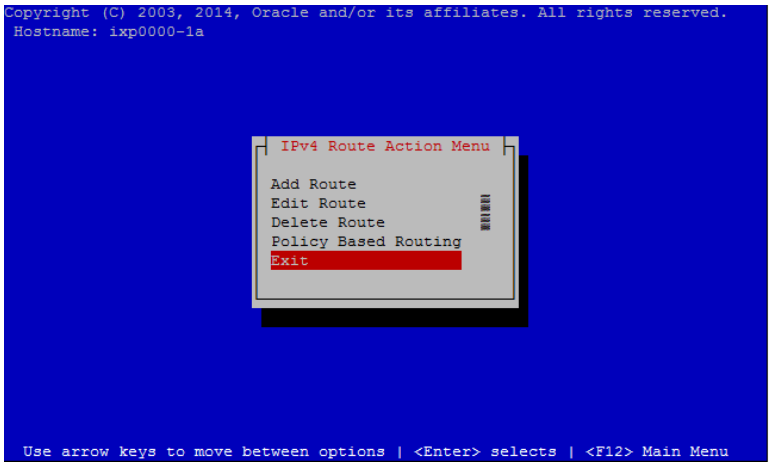
10	Select IPv4	press **[ENTER]** to continue. 
11	Select Add address	press **[ENTER]** to continue. 

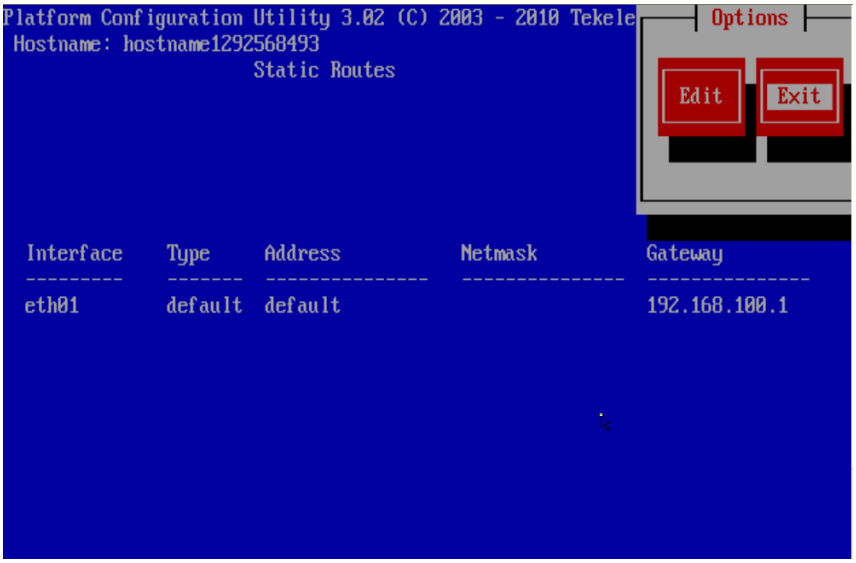
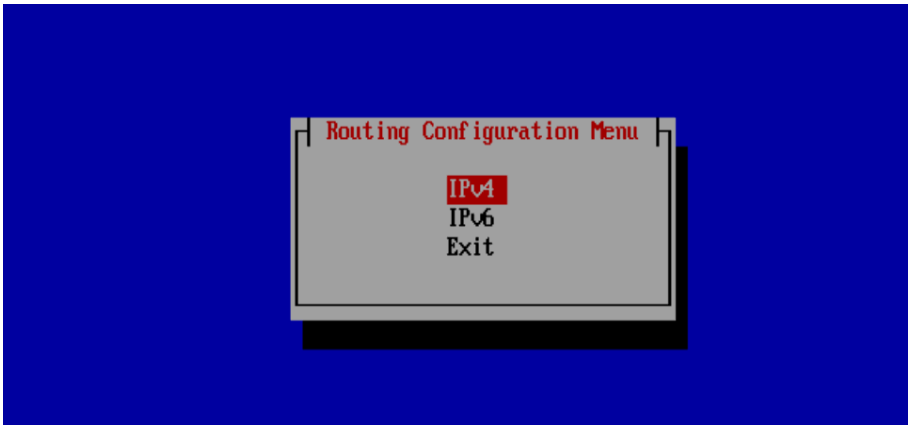
12	Set the IP address and Netmask identified for the eth01 interface	Use the **[TAB]** and arrow keys on the keyboard to add IP address. Enter the IP address of the server then press **[TAB]** to select NETMASK. Press **[TAB]** to select **( ) yes** and press **[SPACEBAR]** to select then **[TAB]** and 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.

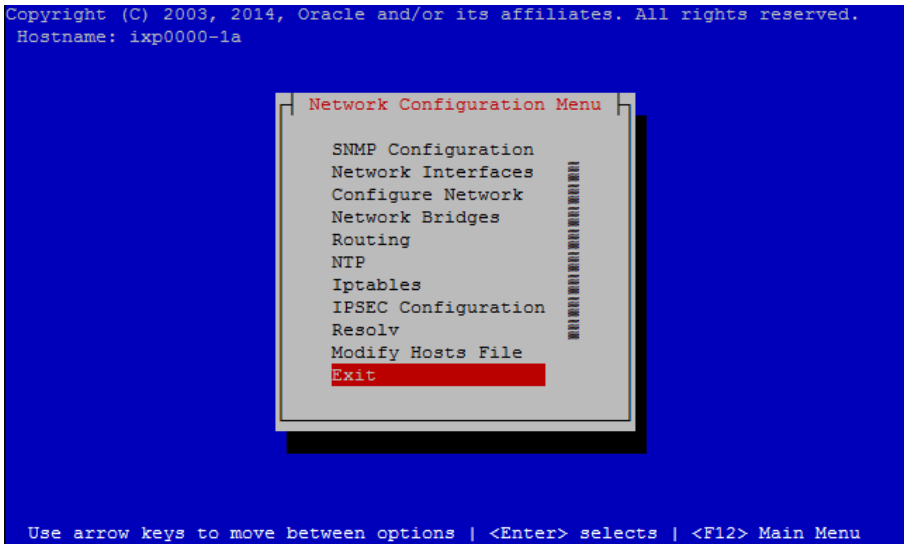
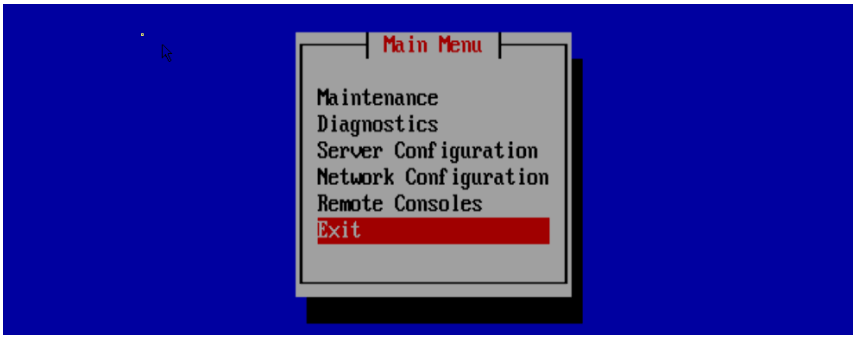
14	Verify the settings and exit	Once the screen comes back, **verify the IP address and Netmask**. Use the **[TAB]** key on the keyboard to select Exit and press **[ENTER]** to continue.  Use the **[TAB]** key on the keyboard to select Exit and press **[ENTER]** to continue  **Expected Result:** IP address 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.

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,10.236.2.141,IXP-PDU,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,IXP-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-BASE,eth01,255.255.255.224,10.236.2.129
```

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,10.236.2.141,IXP-PDU,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,DR-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-BASE,eth01,255.255.255.224,10.236.2.129
```

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:

```
ntpserver1,10.236.129.11
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: 10.236.2.141
- 1b server is the Base Server with the IP address: 10.236.2.142
- 1c server is the Base Server with the IP address: 10.236.2.143
- Network interface: eth01
- Network mask: 255.255.255.254
- Default gateway: 10.236.2.129

• NTP server IP address: 10.236.129.11

• 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,10.236.2.141,IXP-PDU,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,IXP-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-BASE,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
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,10.236.0.33
```

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>
```

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>
```

Example for IMF 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
```

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:

```
ntpserver1,10.236.129.11
```

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
...
```

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: 10.250.32.10
- 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.

```
# 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
ntpserver1,10.250.32.10
ntpserver2,10.250.32.11
ntpserver3,10.250.32.12
ntppeerA,10.250.32.13
ntppeerB,10.250.32.14
nspprimary,10.10.10.10
nspsecondary,10.10.10.11
nsporacle,10.31.2.60
timezone,Europe/Paris
```

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 oinstall.

   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 dir 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

Please refer to KM_1683859.2 for **Capacity Management Good Practices.**

How to configure NTP

Please refer KM_2083591.1 to configure NTP.

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 10.2, 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

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 10.250.70.115 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
```

Appendix D: My Oracle Support

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

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