

Oracle® Communications
Performance Intelligence Center
Upgrade Guide
Release 10.2.1
E77487-02

March 2018

Copyright © 2003, 2018 Oracle and/or its affiliates. All rights reserved.

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notices are applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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



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

Refer to Appendix section for instructions on accessing My Oracle Support and Oracle Help Center.

Table of Contents

- Chapter 1: About This Help Text 1**
- Scope and Audience..... 1
- Related Publications 1
- Requirements and Prerequisites 1
 - Hardware Requirements 1
 - Software Requirements..... 1
- Reference Documents 3
- Chapter 2: Major Upgrade Overview Flowcharts..... 4**
- Performance Intelligence Center High-level Major Upgrade 4
- Packaging Major Upgrade Overview 6
- Management Server Upgrade Overview 6
- Acquisition Major Upgrade Overview..... 7
- Mediation Server Major Upgrade Overview 8
- Chapter 3: Major Backout Overview Flowcharts 9**
- Management Server Major Backout..... 9
- Acquisition Server Major Backout 9
- Mediation Server Major Backout..... 9
- Chapter 4: Healthcheck..... 10**
- Mediation Subsystem Healthcheck 10
- Acquisition Server Healthcheck 12
- Management Server Pre-Upgrade Healthcheck and Settings 14
- Global Healthcheck..... 20
- Chapter 5: Management Server Major Upgrade 22**
- Upgrade setup 22
- Post-Upgrade Settings 22
- Management Server Post-Upgrade Check..... 24
- Management Server Backup..... 25
- Upload xDR Builder ISO to Management Server 26
- Chapter 6: Acquisition Server Major Upgrade 29**
- Acquisition Server Pre-Install Configuration..... 29
- Acquisition Server Pre-Install Healthcheck..... 30

Install Acquisition Server	30
Sync Management Server with Acquisition Server.....	31
Acquisition Server Post-Sync Healthcheck	33
Chapter 7: Mediation Server Major Upgrade.....	36
Install Operating system	36
Mediation Server Pre-Install Configuration.....	36
Install Mediation Server.....	39
Mediation Server Post-Install Healthcheck	40
Integrate Customer Network.....	41
Install xDR Builders	42
Mediation Subsystem Healthcheck	44
Upgrade DTO Package	47
Mediation Server Post-Integration Configuration	49
Chapter 8: Knowledge Base Procedures	51
ReInstall Operating system	51
How To Mount the ISO file from PM&C ISO Repository.....	51
Adding ISO Images to the PM&C Image Repository	53
How to connect a server console using iL0 ssh connection	53
PM&C upgrade.....	54
Update the switch configurations	54
Unset Configuration on Management Server.....	55
Chapter 9: Management Server Backup (Post Upgrade)	56
Appendix A: My Oracle Support.....	57

List of Figures

Figure 1. High level upgrade	5
Figure 2. Management Server Major Upgrade.....	6
Figure 3. Acquisition Major Upgrade.....	7
Figure 4. Mediation Major Upgrade	8

Chapter 1: About This Help Text

Scope and Audience

This document describes the major upgrade procedures for the "Oracle Communications Performance Intelligence Center" system at Release **10.2.1**, also referred to as "**considered**" release in this document.

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 the considered release.

Requirements and Prerequisites

Hardware Requirements

Please refer to [Hardware Guidelines](#), of the considered release.

Software Requirements

The following software is required for the considered release upgrade.

Take in consideration you might need also the software from the installed release in case you would have to proceed a disaster recovery. Refer to Performance Intelligence Center **10.2** maintenance guide for detailed instruction.

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](#)

Note: For specific versions and part numbers, see the Performance Intelligence Center Release Notice.

The following software is required for the Performance Intelligence Center 10.2 upgrade.

Oracle Communication GBU deliverables:

- Management Server
- Mediation Server
- Mediation Protocol
- Acquisition Server
- Acquisition Datafeed
- TPD

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

<https://edelivery.oracle.com/>

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
Patches for Oracle Communications Performance Intelligence Center	KM_1989320.2
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

In case of engineered system like ODA and ZFS the upgrade of its software is not mandatory, however in case customer want to update ODA or ZFS software following information can be used:

- ODA
 - Oracle Database Appliance - 12.1.2 and 2.X Supported ODA Versions & Known Issues [KM_888888.1](#)

- As reminder, the initial installation documentation is there [Database Appliance Getting Started Guide](#)
- ZFS
 - Oracle ZFS Storage Appliance: Software Updates [KM_2021771.1](#)
 - As reminder, the initial installation documentation is there [ZFS Storage Appliance Installation Guide](#) and [ZFS Storage Appliance Administration Guide](#) .

Reference Documents

- [1] [Platform Configuration Guide](#), Tekelec Platform release 7.4
- [2] [TPD Initial Product Manufacture](#), Tekelec Platform release 7.4
- [3] [PM&C Incremental Upgrade](#), Tekelec Platform release 7.4
- [4] [HP Solutions Firmware Upgrade Pack 2.2.10](#), Tekelec Platform release 7.4
- [5] [Oracle Firmware Upgrade Pack](#), Tekelec Platform release 7.4
- [6] [Teklec Default Passwords, CGBU_ENG_24_2229 \(restricted access, refer to Appendix A: My Oracle Support\)](#)
- [7] [Performance Intelligence Center Hardware Guidelines](#), release 10.2.1
- [8] [Performance Intelligence Center Security Guide](#), release 10.2.1
- [9] [Performance Intelligence Center Release Notice](#), release 10.2.1
- [10] [Performance Intelligence Center Patch Installation Guide](#), release 10.2.1, (formely Incremental Upgrade)
- [11] [Performance Intelligence Center Installation Guide](#), release 10.2.1
- [12] [Performance Intelligence Center Maintenance Guide](#), release 10.2.1 and release 10.2

Chapter 2: Major Upgrade Overview Flowcharts

Performance Intelligence Center High-level Major Upgrade

This flowchart describes the Performance Intelligence Center high-level major upgrade overview. Referring to the graphic below the applicable order of each component is depicted and for each component the applicable flowchart is identified by section of this document where it is located.

Described major upgrade procedures are applicable to systems installed in 10.2.0 release. Following this procedure, the system will be upgraded to 10.2.1 release

It is recommended to upgrade the firmware needs to the latest Oracle supported levels for all hardware components, however this firmware upgrade is not mandatory.

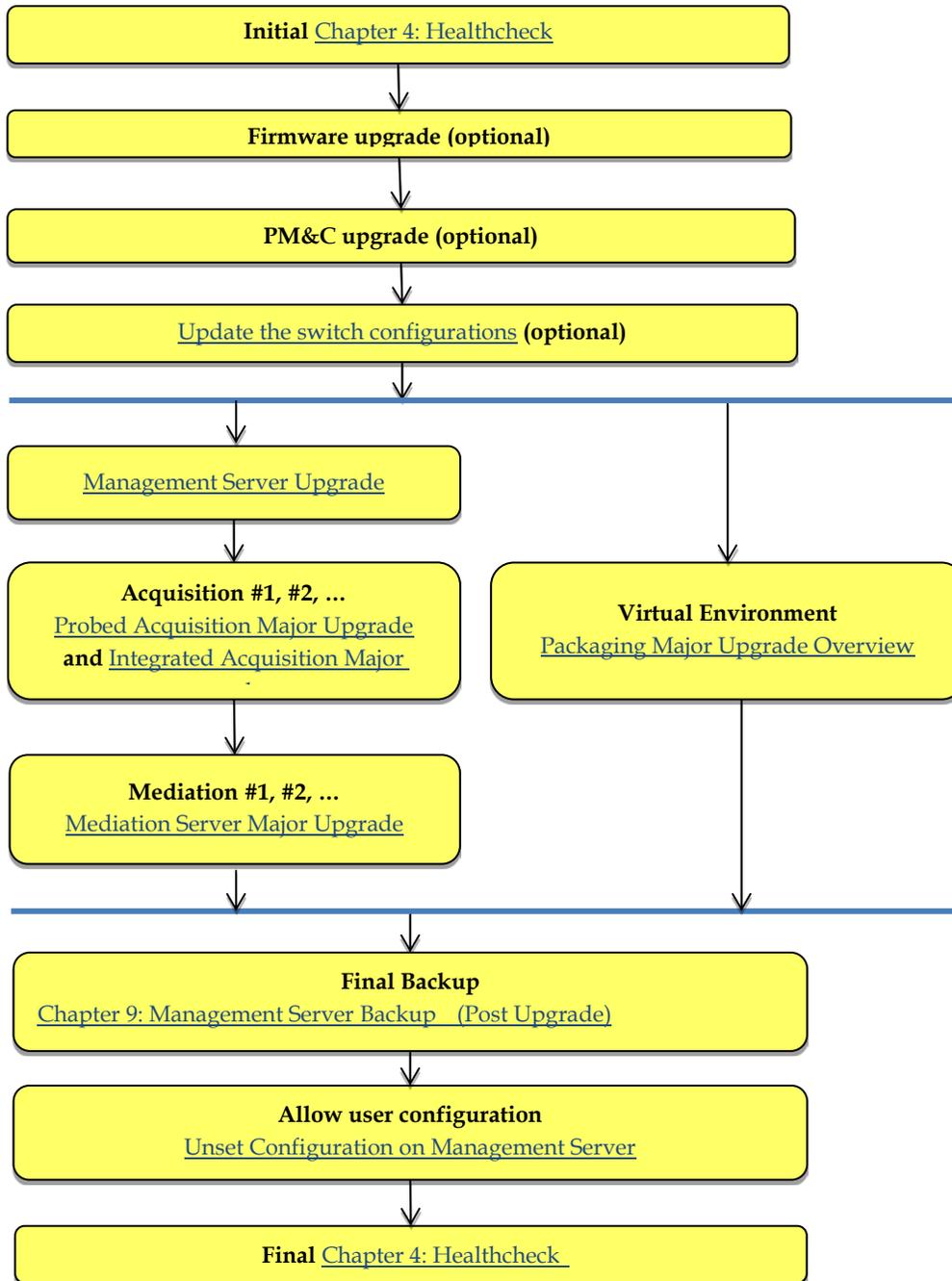
The system on the source release may install all patches applicable to source release prior the major upgrade, but it is not mandatory. However once the system is updated to target release it is mandatory to apply all the available necessary patches.

The patches are available at MOS [KM_1989320.2](#)

Note:

1. Initial health check at least 2 weeks before the planned operation in order to have time to replace defective hardware
2. Optional Firmware upgrade to the latest release available.
3. PM&C Platform upgrade for potential security fixes

Figure 1. High level upgrade



Packaging Major Upgrade Overview

This chapter covers packages combining multiple Performance Intelligence Center components in a Virtual Environment.

These packages are for the “Integrated DSR Monitoring Prepackage” and for any customized packaging compliant with the [Installation Guide](#), of the release 10.2.0.

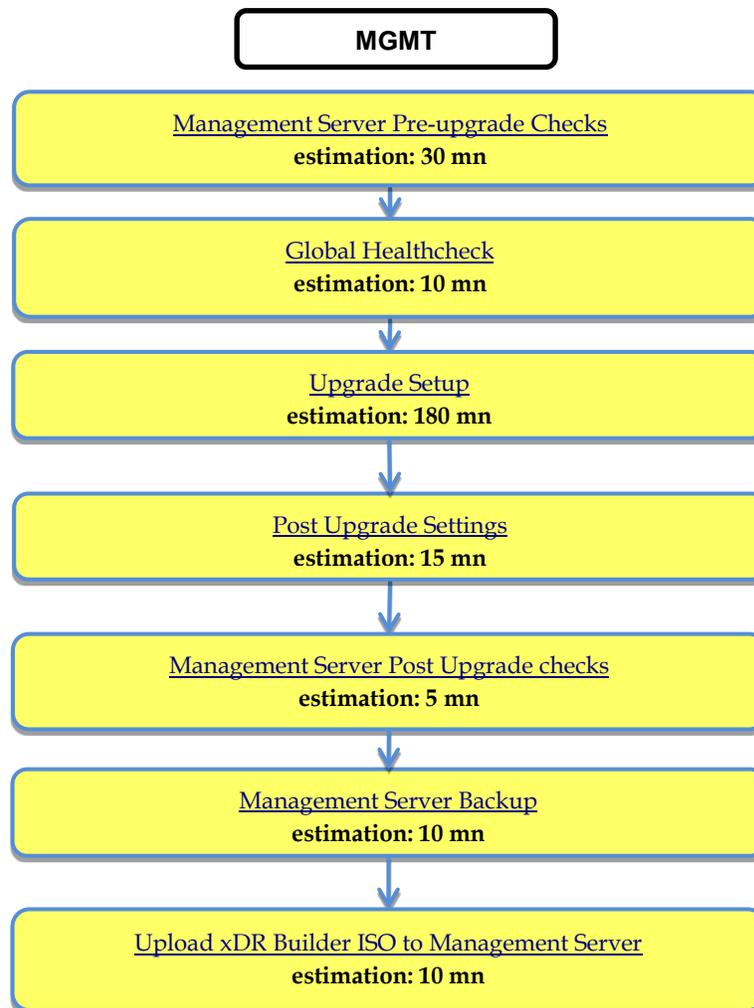
All components are upgraded individually in their own individual Virtual Machine, considered as the host of each component. In other words, the same approach than for legacy installation can be applied

Management Server Upgrade Overview

The major upgrade on MGMT standard server shall use the IPM strategy, where the system will be re-installed with latest release and configuration backup is restored during the procedure.

The upgrade procedure is valid for both configurations of previous release (10.2) on TPD based or on Standard Oracle Linux platform

Figure 2. Management Server Major Upgrade



Acquisition Major Upgrade Overview

This flowchart depicts the sequence of procedures that must be executed to upgrade standalone Probed Acquisition Server and Integrated Acquisition subsystem.

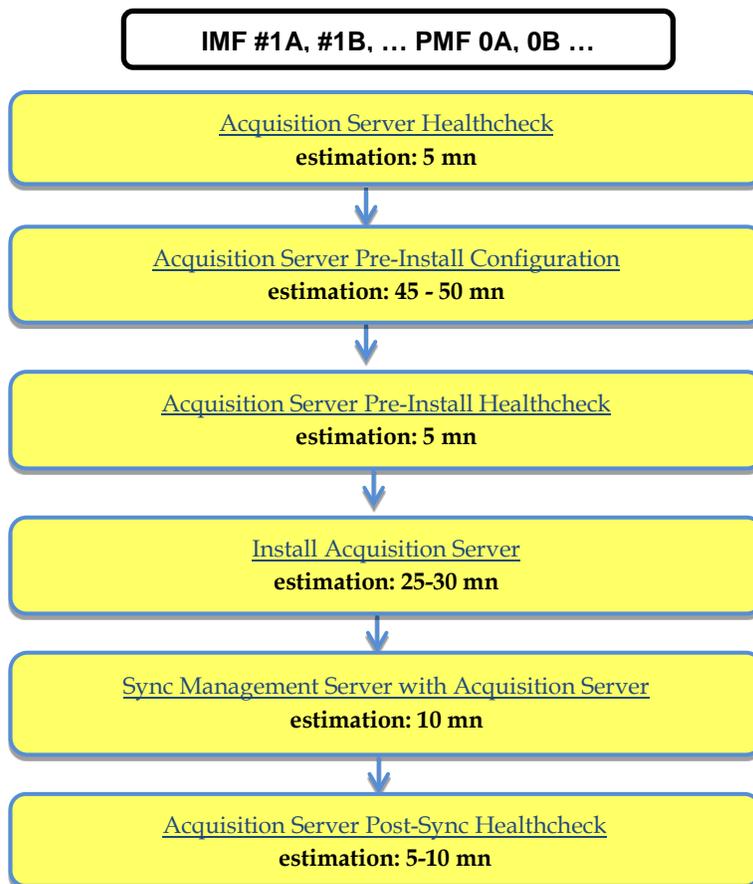
For **Integrated DSR Monitoring** based on Probed Acquisition, proceed in the same manner.

Depending on the number of servers for a particular function, the required procedures depicted in the flowchart will need to be repeated.



CAUTION: This procedure is introducing some data loss for the customer.

Figure 3. Acquisition Major Upgrade



Mediation Server Major Upgrade Overview

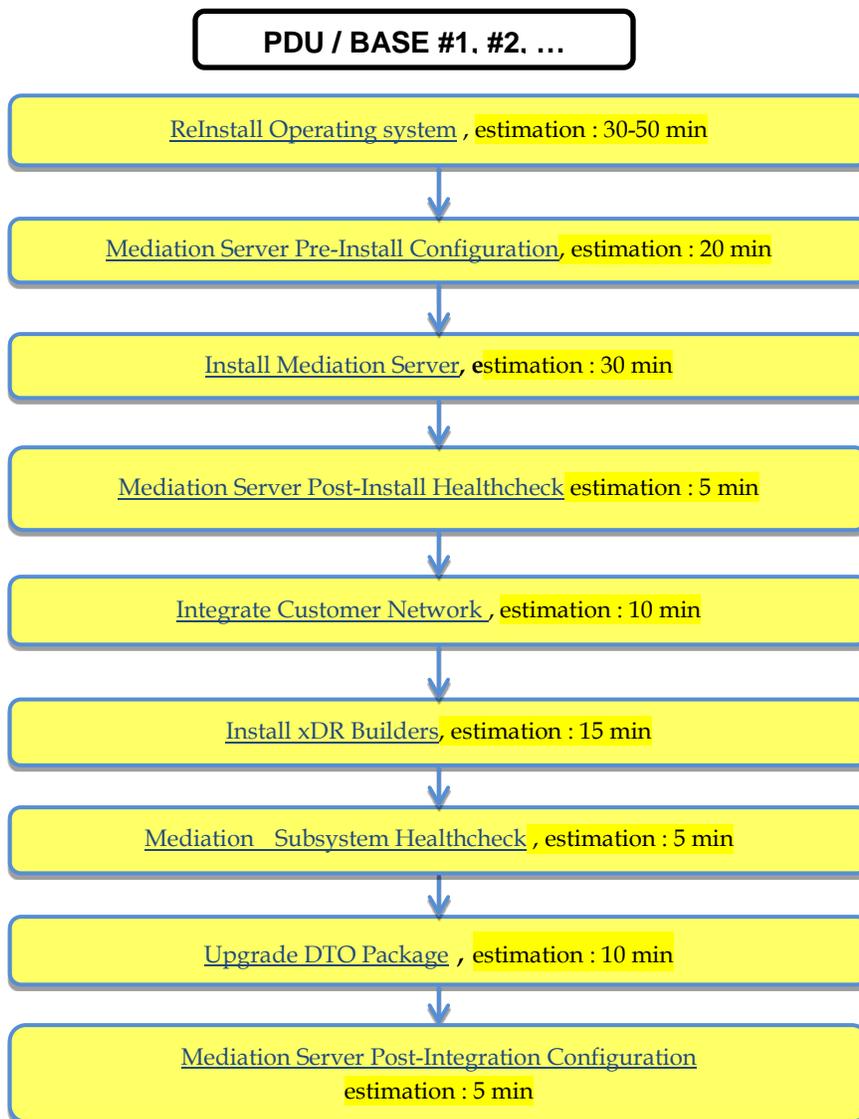
This flowchart depicts the sequence of procedures that must be executed to upgrade the Mediation subsystem and associated server functions.

The Mediation subsystem consists of the following types of servers at the beginning of the procedure:

- Mediation PDU storage server (not existing for Mediation freshed installed in 10.2)
- Mediation Base server

Mediation subsystem major upgrade procedure is triggered from each server in the subsystem manually but runs in parallel on all servers in the subsystem.

Figure 4. Mediation Major Upgrade



Chapter 3: Major Backout Overview Flowcharts

The **backout** is design to come back to the previous release. It will be done using the DR procedures of the source release installed, [Maintenance Guide](#) of Release 10.2.0

Management Server Major Backout

NSP application major backout is implemented as a Disaster Recovery procedure. Follow maintenance guide of the source release to find a Disaster Recovery Procedure.

Acquisition Server Major Backout

Acquisition application major backout is implemented as a Disaster Recovery procedure. Follow maintenance guide of the source release to find a Disaster Recovery Procedure.

Mediation Server Major Backout

Mediation application major backout is implemented as a Disaster Recovery procedure. Follow maintenance guide of the source release to find a Disaster Recovery Procedure.

Mediation Subsystem Healthcheck

This procedure describes how to run the automatic healthcheck of the Mediation subsystem, including connectivity to the DWS:

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:

```
[cfguser@ixp2222-1a ~]$ analyze_subsystem.sh
----- ANALYSIS OF SERVER ixp2222-1a STARTED
-----
10:16:05: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
10:16:05: date: 05-20-11, hostname: ixp2222-1a
10:16:05: TPD VERSION: 4.2.3-70.86.0
10:16:05: IXP VERSION: [7.1.0-54.1.0]
10:16:05: XDR BUILDERS VERSION: [7.1.0-36.1.0]
10:16:05: -----
10:16:05: Analyzing server record in /etc/hosts
10:16:05:      Server ixp2222-1b properly reflected in /etc/hosts file
10:16:05: Analyzing IDB state
10:16:05:      IDB in START state
...
12:21:48: Analyzing disk usage
...
10:24:09: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp2222-1b

ixp2222-1a TPD:[ 4.2.3-70.86.0 ] IXP:[ 7.1.0-54.1.0 ] XB:[ 7.1.0-36.1.0 ]  0
test(s) failed
ixp2222-1b TPD:[ 4.2.3-70.86.0 ] IXP:[ 7.1.0-54.1.0 ] XB:[ 7.1.0-36.1.0 ]  0
```

test(s) failed

Example of a successful test:

10:24:08: Analyzing DaqServer table in IDB

10:24:08: Server ixp2222-1b reflected in DaqServer table

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

Open a terminal window and log in as cfguser on any Mediation Server in the Mediation subsystem and use the following command to have the list of the DatawareHouse

```
[cfguser@ixp0101-1a ~]$ Imysql.client
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 16501
Server version: 5.1.66 Source distribution

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select concat(Login , '/' , Password , '@' , Host , '/' , Instance) from DatawareHouse;
+-----+
| concat(Login , '/' , Password , '@' , Host , '/' , Instance) |
+-----+
| IXP/IXP@10.253.142.203/IXP                                     |
| IXP/IXP@10.253.142.204/IXP                                     |
+-----+
1 row in set (0.01 sec)

mysql> exit
```

Then, for each line, make sure that the database is accessible by using the following command:

```
[cfguser@ixp0101-1a ~]$ sqlplus IXP/IXP@10.253.142.203/IXP

SQL*Plus: Release 11.2.0.2.0 Production on Thu Sep 11 04:57:14 2014

Copyright (c) 1982, 2010, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Data Mining
and Real Application Testing options

SQL> exit
```

Note: Some of the xDR/KPI sessions are stored on different servers in the xDR Storage pool. As Centralized xDR Builder upgrade is analyzing all session that are configured on particular Mediation subsystem, all Oracle servers where those sessions are stored must be accessible. Otherwise Centralized xDR Builder upgrade will fail.

Acquisition Server Healthcheck

This procedure describes how to run the health check script on Acquisition servers.

The script gathers the health check information from each server in the Integrated Acquisition subsystem or from Probed Acquisition server. The script should be run from only on one server of the Integrated Acquisition subsystem (the 1A server is preferred) or on stand-alone. The output consists of a list of checks and results, and, if applicable, suggested solutions.

1. Run the automatic healthcheck script and verify output
 - a. Run analyze_subsystem.sh script as cfguser:

```
$ analyze_subsystem.sh
```
 - b. 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 A: My Oracle Support](#)

Note: For a standalone, there will be only one server in the output. Example output for a healthy subsystem:

```
-----
ANALYSIS OF SERVER IMF0502-1A STARTED
-----

11:28:59: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
11:28:59: date: 02-07-11, hostname: IMF0502-1A
11:28:59: TPD VERSION: 3.3.8-63.25.0
11:28:59: XMF VERSION: [ 60.6.7-2.1.0 ]
```

```
11:28:59: -----
11:28:59: Checking disk free space
11:28:59:      No disk space issues found
...
11:29:08: Checking whether ssh keys are exchanged among machines in frame - this can
take a while
11:29:08:      3 mates found: yellow-1B yellow-1C yellow-1D
11:29:26:      Connection to all mates without password was successful
11:29:26: Checking A-Node server
11:29:29:      Connection to A-Node 10.240.9.4 was successful
11:29:29:      A-Node version is: 60.6.7-2.1.0
11:29:29: Checking version of the nsp
11:29:32:      Connection to nsp 10.240.9.3 was successful
11:29:32:      nsp version is: 6.6.4-7.1.0
11:29:32:      nsp was installed on: 2011-01-13 05:09:26 (25 days 6 hours ago)
11:29:32: All tests passed. Good job!
11:29:32: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0502-1A
```

```
-----
ANALYSIS OF SERVER IMF0502-1B STARTED
-----
```

```
...
...
11:30:04: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0502-1B
```

```
-----
ANALYSIS OF SERVER IMF0502-1C STARTED
-----
```

```
...
...
11:30:36: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0502-1C
```

```
IMF0502-1A  TPD: 3.3.8-63.25.0  XMF: 60.6.7-2.1.0  0 test(s) failed
IMF0502-1B  TPD: 3.3.8-63.25.0  XMF: 60.6.7-2.1.0  0 test(s) failed
IMF0502-1C  TPD: 3.3.8-63.25.0  XMF: 60.6.7-2.1.0  0 test(s) failed
```

Example output for a subsystem with errors:

```
...
...
END OF ANALYSIS OF SERVER IMF0502-1D
```

```
IMF0502-1A TPD: 3.3.8-63.25.0 XMF: 60.6.7-2.1.0 1 test(s) failed IMF0502-1B TPD:
3.3.8-63.24.0 XMF: 60.6.7-1.0.0 3 test(s) failed server on interface yellow-1c is not
accessible (ping)
IMF0502-1D TPD: 3.3.8-63.25.0 XMF: 60.6.7-2.1.0 0 test(s) failed
Differences between tpd platform versions found!
Differences between message feeder application versions found!
```

Management Server Pre-Upgrade Healthcheck and Settings

This procedure describes pre-upgrade checks on Management Server together with a few configuration settings.

Note: In Final Health Check, this procedure must be skipped.

1. Builder Upload and Dry Run

This step is added as a pre-upgrade check to inform user about possible removal of dictionary fields that impact the queries and filters. In this step, it is only recommended to install new xdr builder RPM on management server when it is still on previous release and execute the Dry Run report from upgrade utility.

I. Install Builder ISO on Management Server

- a. Copy the xDR builder ISO to the Management Server primary Weblogic server or insert xDR Builder CD-ROM.
- b. Login to the Management Server.
- c. As root run:

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

- d. You will be prompted:
Please enter path to Builder CDROM or ISO [/media/cdrom]
- e. Choose one of the following:

- If you have used ISO file enter the exact path including the ISO name
- If you have used CDROM press <ENTER>

- f. Wait until installation finishes.

II. Verification of ISO installation on Management Server.

- a. Login to the NSP application interface as TklcSrv user.
- b. Click Upgrade Utility
- c. Click on Manage Builder Rpm on the left tree.

It will display the list of the xDR builder rpm. One of them is the one that belongs to the ISO file installed in the previous step. The state will be Not Uploaded.

The list will also display the supported platform of the builder ISO file. The supported platform can be "32 bit", "64 bit" or "32,64 bit". The supported platform "32,64 bit"

means that same version of builder ISO has been installed twice, one that supports 32 bit and the other that supports 64bit.

III. Dry run

- a. Login to the NSP GUI as TkIcSrv user.
- b. Launch Upgrade Utility
- c. Click on Manage Builder Rpm on the left tree.

It will display the list of the xDR builder rpm. Select the RPM which you want to upgrade and choose **Dry Run** option from the tool bar.

- d. Dry Report will be generated for each dictionary indicating changes done on the new dictionaries (Added/Removed/Deprecated field(s))

This report is just an information at this time but will be very useful to finalize the upgrade and to prepare in advance what would be required to be done. It will also display the name of the configuration which are using deprecated field and configurations which will become incompatible after removal of field.

If there are configurations (Query/Protraq/xDR filter) on the removed field, then modify those configurations to remove the use of removed field. Otherwise those configurations will be removed from the NSP when you upload the builder RPM.

The dry run can't anymore be executed once the new package would be installed on the Mediation subsystem but you would have access to similar information on the deprecated fields menu you can access from the utility home page.

IV. Uninstall the Builder RPM from management server

- a. Login to the NSP GUI asTkIcSrv user and Launch Upgrade Utility
- b. Click on Manage Builder Rpm on the left tree.
- c. It will display the list of the xDR builder rpm. Select the RPM which was used for dry run and click the delete option from the tool bar.

2. Performance Intelligence Center backup

The main goal of this step is to make sure that for upgrade latest backup is taken and backup must contain the global backup. The latest backup shall already contain the global backup so the latest available nightly backup can be used, however it is always recommended to take the global backup manually.



Make sure that before the backup is taken all the pending configuration changes are applied and if not then apply the configuration changes.

Go to the path /opt/nsp/scripts/oracle/cmd and run the below script.

```
# sh launch_pic_global_backup.sh
```

Note: The script will prompt for the Management DB password during execution. Please provide the DB password.

The above script will take the Management Server backup on one box server or oracle box server along with the Mediation Server/Acquisition Server backup at path /opt/oracle/backup/NSP_BACKUP_XX_XX_XX_XX_XX_XX

Note: Please verify export realm directory inside upgrade_backup (/opt/oracle/backup/upgrade_backup/exportrealm) directory on one box server or primary box server that its content has latest timestamp (approximately the same timestamp when the latest backup folder was created).



Any changes done after the backup will be lost!

3. Check Management Server Backup is valid

This procedure describes different steps to be followed for checking the backup of Management Server is valid. It is useful to have this backup in case of restoring the setup need arising from upgrade failure

There must be one directory for the last seven days and it is recommended to copy in a safe place the full content of at least the last of this directory.

```
# cd /opt/oracle/backup
# ls -lh
drwxrwxrwx 9 root  root      4096 Jun 28 22:01 NSP_BACKUP_06_28_12_22_00_01
drwxrwxrwx 9 root  root      4096 Jun 29 22:01 NSP_BACKUP_06_29_12_22_00_02
drwxrwxrwx 9 root  root      4096 Jun 30 22:01 NSP_BACKUP_06_30_12_22_00_01
drwxrwxrwx 9 root  root      4096 Jul  1 22:01 NSP_BACKUP_07_01_12_22_00_01
drwxrwxrwx 9 root  root      4096 Jul  2 22:01 NSP_BACKUP_07_02_12_22_00_01
drwxrwxrwx 9 root  root      4096 Jul  3 22:01 NSP_BACKUP_07_03_12_22_00_01
drwxrwxrwx 9 root  root      4096 Jul  4 22:01 NSP_BACKUP_07_04_12_22_00_01
```

- a. Check whether the Management Server backup is on external drives or not.

Login as root on Management Server and execute below commands.

```
# cd /opt/oracle/backup
# df -h .
Filesystem                Size  Used Avail Use% Mounted on
/dev/sdd1                  275G  1.1G  274G   1% /usr/TKLC/oracle/backup
```

The outputs shown above are examples but they shows that /usr/TKLC/oracle/backup directory is mounted on /dev/mapper/nsp_backup_vol partition in case of blade machines or on /dev/sdd1 partition in case of RMS machines. These partitions are on

external storage array. If the output is not similar as shown above then do not proceed further and refer to [Appendix A: My Oracle Support](#)

- b. Check the content of the last backup directory

```
-rw-r--r-- 1 root root 391K Mar 24 22:01 apache-conf.tgz
-rw-r--r-- 1 root root 169 Mar 24 22:01 backup.log
-rw-r--r-- 1 root root 186 Mar 24 22:00 boot.properties
drwxr-xr-x 10 root root 4.0K Mar 24 22:00 config
-rw-r--r-- 1 root root 6.9K Mar 24 22:01 customer_icon.jpg
-rw-r--r-- 1 oracle oinstall 3.0M Mar 24 22:01 ExpNSP.dmp.gz
-rw-r--r-- 1 oracle oinstall 52K Mar 24 22:01 ExpNSP.log
drwxr-xr-x 2 root root 4.0K Mar 24 22:00 exportrealm
-rw-r--r-- 1 root root 230k Mar 24 22:01 failedconnection.txt
-rw-r--r-- 1 root root 2.5K Mar 24 22:01 global_versions.properties
-rw-r--r-- 1 root root 235 Mar 24 22:01 hosts
-rw-r--r-- 1 root root 1585 Mar 24 22:01 hosts.csv
-rw-r--r-- 1 root root 163 Mar 24 22:01 ifcfg-eth01
-rw-r--r-- 1 root root 23 Mar 24 22:01 ifcfg-eth02
-rw-r--r-- 1 root root 47K Mar 24 22:01 install.log
drwxrwxrwx 2 root root 4096 Mar 24 22:01 IXP
-rw-r--r-- 1 root root 59M Mar 24 22:01 jmxagentproperties.tgz
drwxr-xr-x 7 root root 4.0K Mar 24 22:00 ldap
-rw-r--r-- 1 root root 85 Mar 24 22:01 network
-rw-r--r-- 1 root root 600 Mar 24 22:01 nsp_setenv.sh
-rw-r--r-- 1 root root 1.6K Mar 24 22:01 ntp.conf
-rw-r--r-- 1 root root 298 Mar 24 22:01 optional_modules_list
-rw-r--r-- 1 root root 320 Mar 24 22:00 preBackupTests.log
-rw-r--r-- 1 root root 148 Mar 25 05:44 restore_10.248.19.35.log
-rw-r--r-- 1 root root 64 Mar 24 22:00 SerializedSystemIni.dat
-rw----- 1 root root 0 Mar 24 22:01 snmpd.conf
drwxrwxrwx 2 root root 4096 Mar 24 22:01 XMF
```

Make sure the file ExpNSP.dmp.gz exist and have a size coherent with the amount of data of your customer. Check the content of ExpNSP.log

Check the content of **Mediation** backup folder

```
-rw-r--r-- 1 root root 610 Mar 24 22:01 IXP_ixp1000-1a.tgz
-rw-r--r-- 1 root root 645 Mar 24 22:01 IXP_ixp1000-1b.tgz
-rw-r--r-- 1 root root 560 Mar 24 22:01 IXP_ixp1000-1z.tgz
```

Copy following file manually from all the servers in mediation sub-system and keep inside mediation backup for individual servers

/usr/TKLC/TKLCixp/prod/lib/plugins/build/SCTPPathNaming.cnf

Check the content of **Acquisition** backup folder

Verify that global_version.properties file must be present in the latest backup directory, verify that

- a. global_version.properties file inside the latest backup directory.
- b. ExpNSP.dmp.gz file should not be empty and check no errors in the content of ExpNSP.log
- c. In exportrealm directory four files i.e. DefaultAuthenticator.dat, DefaultCredentialMapper.dat, XACMLAuthorizer.dat, XACMLRoleMapper.dat should be present
- d. Copy the SSL certificates if present on the server and keep them into backup directory /opt/oracle/backup/NSP_BACKUP_XX_XX_XX_XX_XX_XX

Note:The above certificates must be restored manually after the management server upgrade to prevent warning about the SSL certificate error in case of https access.

- e. run healthcheck:

For the ISO file, run:

```
# sh /mnt/upgrade/health_check/healthcheck_nspbackup.sh
```

```
[root@nsp9 health_check]# sh healthcheck_nspbackup.sh
Last NSP backup is /opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01
Verifying expected files in /opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01
directory
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/jmxagentproperties.tgz File
exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/bulkconfig File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ExpNSP.dmp.gz File exists
[ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/hosts File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ifcfg-eth0 File does not exists
[ NOT OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ifcfg-eth1 File does not exists
[ NOT OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ifcfg-eth01 File does not exists
[ NOT OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ifcfg-eth02 File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ifcfg-bond0.3 File exists
[ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ifcfg-bond0.4 File does not
exists [ NOT OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/network File exists [ OK ].
```

```

/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/nsp_setenv.sh File exists
[ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ntp.conf File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/optional_modules_list File
exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/snmpd.conf File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/apache-conf.tgz File exists
[ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/expoortrealm/DefaultAuthenti
cator.dat File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/expoortrealm/DefaultCredenti
alMapper.dat File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/expoortrealm/XACMLAuthori
zer.dat File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/expoortrealm/XACMLRoleMa
pper.dat File exists [ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/customer_icon.jpg File exists
[ OK ].
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/global_versions.properties
File exists [ OK ].
Verifying size of NSP DMP file
/opt/oracle/backup/NSP_BACKUP_03_30_14_22_00_01/ExpNSP.dmp.gz file size is
[ OK ]
Health check complete

```

Note: In above example eth01 & eth02 interface will be present in case of RMS and ifcfg-bond0.3 && ifcfg-bond0.4 will be available in case of blade server. Note that Blade is no more supported in this release.

f. Copy backup directory

- i. Login as a root user on Management Server.
- ii. Verify the Management Server backup on which the healthcheck was performed is present and is the latest backup. Execute the below command to find out the latest backup directory:

```

# ls -ltr /opt/oracle/backup/NSP* | tail -1
/opt/oracle/backup/NSP_BACKUP_09_03_14_22_00_01

```

In case of any discrepancy, don't proceed further and refer to [Appendix A: My Oracle Support](#).

- iii. Verify the size of Management Server backup & space available on external server to be used for storing backup.

Command to verify the size of the backup:

```

# du -sh /opt/oracle/backup/NSP_BACKUP_XX_XX_XX_XX_XX_XX
89M      /opt/oracle/backup/NSP_BACKUP_09_03_14_22_00_01

```

Command to verify the available space on the external server, where the backup is to be copied:

```
# Login to the server as root
# df -kh
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root 1008M 333M 625M 35% /
tmpfs                     20G    0  20G  0% /dev/shm
/dev/sda1                  248M   41M 196M 18% /boot
/dev/mapper/vgroot-plat_tmp 1008M  43M 915M  5% /tmp
/dev/mapper/vgroot-plat_usr  4.0G  2.6G 1.2G 69% /usr
/dev/mapper/vgroot-plat_var 1008M 184M 774M 20% /var
/dev/mapper/vgroot-plat_var_tklc 7.9G  6.3G 1.3G 84% /var/TKLC
/dev/mapper/vgroot-plat_nsp  237G  20G 205G  9% /usr/TKLC/nsp
/dev/mapper/vgroot-plat_oracle 7.9G  4.4G 3.2G 59% /usr/TKLC/oracle11
```

Select the partition where the sufficient space is available for the backup and use that partition for copying. The above output is just the sample output and it can be different depending on the external server used.

- iv. Copy the latest backup folder on the external server at the path identified in the previous step, using below command

```
# scp -r /opt/oracle/backup/NSP_BACKUP_XX_XX_XX_XX_XX_XX <Server IP>/<Directory_Path>
```

Global Healthcheck

Note: In Final Health Check, this procedure must be skipped.



CAUTION: Make sure you can access the iLO/iLOM interface of all servers and you can open the remote console for each server. The software installation through SSH is blocked and it can be done only on the server console itself or using iLO for HP servers and iLOM for Oracle servers.

1. System Cleanup

Discuss with the customer to clean up the system as much as possible in order to reduce the risk and avoid any issue due to some objects that would no more be used.

2. Engineering Document

Make sure you get the latest available engineering document and it is up to date.

The latest version should be documented on the Customer Info Portal, as well as the current password for the admin users

3. xDR Session Status

Navigate from the home screen to Troubleshooting Application

NOTE: Look for any sessions that are lagging behind the current time.

- a. View All records
- b. Filter by end date
- c. End date must be the correct time
- d. Screen capture the information

Verify which sessions are lagging.

Statistics sessions must also be considered but take in consideration records are periodically generated.

Try to access the session it-self and check the session content and especially make sure the PDU are properly recorded.

4. Systems Alarms

Access the system alarm and fix all alarms on the system. In case some alarms can't be fixed due to overloaded system for example, the remaining alarms before the upgrade must be captured in order to compare with the alarms we would get at the end of the upgrade.

5. Alarm Forwarding

Connect on Management Server and Navigate in platcfg menu to check the SNMP and SMTP configuration.

Make sure the SNMP and SMTP configuration are up to date in the Engineering Document.

6. KPI Application

Access to KPI configuration and check which configuration are NOT-SYNC

7. Dashboard

Access to Dashboard configuration and check each dashboard is working fine

8. DataFeed

Access to the DataFeed configuration and capture the Feed Status

Make sure each Feed configuration is Documented in the Engineering Document

9. Scheduler

Access to the Scheduler and check the scheduled tasks configured are working as expected.

Make sure each task is documented in the Engineering Document.

Chapter 5: Management Server Major Upgrade

This section provides the procedures for upgrading the Applications.

Upgrade setup

1. Check Management Server Backup

Note: This is the time user can copy the verified backup from the external server to this server, if not already present.

- a. Login as root user on the server.
- b. Verify the Management Server backup on which the healthcheck was performed using “section **Check Management Server Backup is valid** “ is present and is the latest backup. Execute the below command to find out the latest backup directory:

```
# ls -ltr /opt/oracle/backup/NSP* | tail -1  
/opt/oracle/backup/NSP_BACKUP_09_03_14_22_00_01
```

- c. Change the rights of the Backup before starting the upgrade.

```
# chmod -R 777 /opt/oracle/backup/NSP_BACKUP*
```

In case of any discrepancy, don't proceed with upgrade and refer to [Appendix A: My Oracle Support](#)

2. Reinstall the Management server

Perform steps mentioned in [KM_2164544.1](#)

Note: For virtual environment, refer to section **Management Guest OS reinstallation** in [Installation Guide](#), of the considered release, to install OS.

3. DSR monitoring post-installation

In case of DSR monitoring , refer to section **Installation of Management Server** in [Installation Guide](#), of the considered release, to configure log storage duration.

Refer to section **Creation of Data record** in [Installation Guide](#), of the considered release, to reinstall the small DRS for the Capacity Management.

And refer to section **Creation of PDU Record storage for the use case “troubleshooting”** in [Installation Guide](#), of the considered release

Post-Upgrade Settings

1. Generate DWS and DataFeed Database Credentials(Mandatory)

As root user execute below commands

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

The script shall prompt for the Database Username, Database Service Name, Database IP, old password, new password and wallet password. The credentials provided for DWS server must be same as configured earlier in Management server for the DWS server. This procedure has to be executed individually for each of the DWS servers. The above steps to sync the DWS credentials can be done here i.e after the Management Upgrade or can be done after Upgrade of all OCPIC Components.

2. Restrict access of NSP frontend to HTTPS (Mandatory)

Disable access to HTTP

- a. Open a terminal console and Login as a root user on Management Server One-Box server
- b. Edit /etc/httpd.conf file and search for line "Listen 80"
- c. Remove the line "Listen 80"
- d. Restart httpd daemon
 - a. /bin/systemctl restart httpd.service

3. NSP Applications Documentation

Note: Document for application is automatically installed along with NSP application installation

To verify document installation login into NSP application interface and navigate to **Help ► User Manual** Index page for that application opens. (Each application should be tested and also the link to the PDF should be tested to see if the printable PDF file opens.)

In case you have problems to access some applications such ProTrace, ProTraQ or CCM try to empty you browser cache.

4. Configure Mail Server (Optional)

This procedure describes how to configure the SMTP mail server.

This procedure is optional; however, this option is required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined) and is available only on the Management Server

1. Open a terminal window and log on as root on Standard Server
2. Edit hosts file and make an entry of mail.server as shown below:

```
# vi /etc/hosts
10.248.18.4          mail.server
```

Output of hosts file will be similar as shown below. Replace 10.248.18.4 with your mail server IP

```
# cat /etc/hosts
127.0.0.1 localhost
10.248.18.4          mail.server
```

5. Transfer Ownership of TkclSrv object

Note: Follow the steps only if some object bellowing to TklSrv were created in previous version

- a. Open a web browser and log in to the NSP application interface TkclSrv user.
- b. Navigate to security application ► Transfer ownership value
- c. Transfer all the TkclSrv object to and other user (tekelec for example)

6. Change Customer Icon (Optional)

This procedure describes how to change the customer icon (for example, replace the standard Tekelec logo with a customer logo). This procedure is optional.

- a. Open a terminal window and log in as root on One box.
- b. Copy the customer icon file (customer_icon.jpg) to the /opt/www/nsp/resources directory of respectiver servers.
- c. Verify the customer icon properties:
 - The file name must be customer_icon.jpg.
 - The file must belong to user tekelec in group tekelec.
 - 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.

7. Revoke DBA role from NSP user , see Maintenance Guide of the considered release

8. To enhance alarm description and classification. (Optional)

Note: By default Management Server keep existing alarm classification .

- a. Open a terminal window and log in as root user on Management Server(one box).
- b. Change user to Oracle and execute given command with Management Server database sql user and password.

```
# su - oracle
# sqlplus user/password
@/usr/TKLC/nsp/nsp-package/framework/core/dist/coreDB/sql/CORdb_AlarmEnhancement_data.sql
```

Management Server Post-Upgrade Check

1. Open a terminal window and log in as root on the Management Server
2. As root, run:

```
# /opt/nsp/scripts/procs/post_upgrade_sanity_check.sh
```

Note: When user will execute this script it will automatically accept the upgrade.

3. Review the Management Server installation logs (/var/log/nsp/install/nsp_install.log).

Verify the following:

- Port 80 connectivity is OK
- Oracle server health is OK
- WebLogic health for ports 5556, 7001, 8001 is OK
- 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.

Management Server Backup

This procedure describes how to perform a backup from a Management Server successfully upgraded, in order to avoid restore the backup from previous release in case you would face in issue while the Acquisition Server and Mediation Server upgrade.

```
# ll /opt/oracle/backup/
```

Output should be:

```
drwxrwxrwx 3 oracle oinstall 4096 Apr 8 14:38 upgrade_backup
```

If the permission of /opt/oracle/backup/upgrade_backup is not set as per above snapshot, perform the below step

```
#chmod 777 /opt/oracle/backup/upgrade_backup
```

As root run on management server:

```
# . $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd;  
sh ./launch_pic_global_backup.sh >../trc/cronNSP.log 2>&1
```

This command might take a long time depending on the size of the backup. Refer to the section “**Check Management Server Backup is valid**” in order to make sure everything went fine.

Once the backup is complete, move this backup to some other server. Also make sure the latest backup is the one with which the Major Upgrade was performed.

Path from where backup has to be moved:

```
# /opt/oracle/backup/
```

Note:Edit the cronjob by performing the below steps:

```
#crontab -e
```

Comment out the launch_pic_global_backup.sh entry by putting a hash(#) at the beginning.

You might use the command crontab -l to display the list of jobs scheduled. Below should be the updated entry.

```
# crontab -l
#00 22 * * * . $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd;
sh ./launch_pic_global_backup.sh >./trc/cronNSP.log 2>&1
```

Upload xDR Builder ISO to Management Server

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

Note 1: In case of failure in this step this is not blocking for the Acquisition Server upgrade but only for the Mediation Server. This will give some time to investigate the reason of this over the day. Refer to [Appendix A: My Oracle Support](#).

1. Install Builder ISO on Management Server
 - a. Copy the xDR builder ISO to the Management Server or insert xDR Builder CD-ROM.
 - b. Login to the Management Server

As root run:

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

- c. You will be prompted:

```
Please enter path to Builder CDROM or ISO [/media/cdrom]
```
 - d. Choose one of the following:
 - If you have used ISO file enter the exact path including the ISO name
 - If you have used CDROM press <ENTER>
 - e. Wait until installation finishes.
 2. Verification of ISO installation on Management Server.
 - a. Login to the NSP application interface as TklcSrv user.
 - b. Click Upgrade Utility
 - c. Click on Manage Builder Rpm on the left tree.

It will display the list of the xDR builder rpm. One of them is the one that belongs to the ISO file installed in the previous step. The state will be **Not Uploaded**.

The list will also display the supported platform of the builder ISO file. The supported platform can be "32 bit", "64 bit" or "32,64 bit". The supported platform "32,64 bit" means that same version of builder ISO has been installed twice, one that supports 32 bit and the other that supports 64bit.

3. Dry run

- a. Login to the NSP GUI as TkIcSrv user.
- b. Launch Upgrade Utility
- c. Click on Manage Builder Rpm on the left tree.

It will display the list of the xDR builder rpm. Select the RPM which you want to upgrade and choose **Dry Run** option from the tool bar.

- d. Dry Report will be generated for each dictionary indicating changes done on the new dictionaries (Added/Removed/Deprecated field(s)) and you will have to take in account at the end of upgrade (after section 7.6 Install xDR Builder is completed)

This report is just an information at this time but will be very useful to finalize the upgrade and to prepare in advance what would be required to be done. It will also display the name of the configuration which are using deprecated field and configurations which will become incompatible after removal of field.

If there are configurations (Query/Protraq/xDR filter) on the removed field, then modify those configurations to remove the use of removed field. Otherwise those configurations will be removed from the NSP when you upload the builder RPM.

The dry run can't anymore be executed once the new package would be installed on the Mediation subsystem but you would have access to similar information on the deprecated fields menu you can access from the utility home page.

4. Upload Builder RPM

- a. Mark the requested builder RPM with the Not Uploaded state and press Upload in the toolbar.
- b. A dialog box will appear. Click on Continue to continue the RPM upload.
- c. After the successful upload the RPM state will change 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. View Dictionary Upgrade Status

In case the state of the RPM is “Query/Filter Upgrade Failed”, then the status of upgrade of queries and filters for the dictionaries can be viewed. Below are the steps for the same

- a. Mark the requested builder RPM with the “Query/Filter Upgrade Failed” state and press "Display Dictionary Upgrade Status" button in the toolbar.
- b. Dictionary Upgrade Status will be generated for each upgraded/new dictionary indicating whether the Queries and filters have been upgraded or not for this dictionary.

Chapter 6: Acquisition Server Major Upgrade

The steps mentioned in this chapter must be executed from iLO or similar non disconnectable media.

Acquisition Server Pre-Install Configuration

1. ReInstall Operating system on Acquisition Server



If the PMF is used with a Falco Backup the file `/opt/TKLCmf/prod/falco.conf`

Refer to [Installation Guide](#) of the considered release, first to section **Probed Guest OS reinstallation** and **Probed Guest network** for virtual environment and to section **TPD Installation**, to install OS on the server

2. Acquisition Server Pre-Install Configuration

This section provides procedures to configure the Acquisition servers that must be performed before upgrading the Acquisition application

- a. Temporary Acquisition Server customer IP assignment

Refer to chapter “Manual Configuration of Ethernet Interfaces” from [Maintenance Guide](#), of the considered release

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

- b. Copy ISO

Transfer Application ISO on the server to `/var/TKLC/upgrade` directory

3. Configure Acquisition Server

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

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

Change the current designation and function & hostname

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.

- a. Open platcfg menu using `su - platcfg`
- b. Select Server Configuration->Hostname
- c. Select Edit
- d. Set the hostname
- e. Select Server Configuration -> Designation/Function.

- f. Select Edit.
- g. Change the designation and function.
 - For a Integrated Acquisition subsystem:
In the Designation field, enter the designation in the following format: 1A for the first server, 1B for the second, and so on. In the Function field, enter IMF.
 - For a standalone Probed Acquisition:
In the Designation field, enter the 0A for the server. In the Function field, enter PMF.
- h. Select Exit.

Acquisition Server Pre-Install Healthcheck

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

1. Log in as root on the Acquisition server that you want to install the Acquisition application.
2. Run:


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

Example output for a healthy system:

```
Running modules in class disk... OK
Running modules in class proc... OK
Running modules in class system... OK
Running modules in class hardware... OK
```

```
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

Install Acquisition Server

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

Before you perform this procedure, make sure that you have ISO file available.

1. Log in and copy the ISO file to the server
 - a. Open a terminal window and log in as root on the server that you want to install the Acquisition application.
2. Restore Acquisition Server configuration

Note: in case of DSR Monitoring, as there is no configuration to restore, move on to the next step "Bulkconfig creation".

- a. Log in to the Management Server oracle server as a root user and execute the script as mentioned below

```
# /opt/nsp/scripts/oracle/cmd/restore_ixp_xmf.sh <ip_addr>
```

where `ip_addr` is the ip address of the Acquisition Server on which the restore is to be done.

Note: This script will ask user to provide password for *admusr* and *root*.

- b. Once the script is executed successfully the archive file will be restored at `/var/TKLC/backup/` directory on Acquisition Server.

Note: The installation procedure then take care of restoring the bulkconfig at `/root` directory automatically from the archive file.

3. Bulkconfig creation

Note: this step is to be executed in case of DSR Monitoring only.

- a. Refer to “**Acquisition server bulkconfig file description**” in Appendix B in [Installation Guide](#) of the considered release to create the bulkconfig file.

4. Install the application

- a. Enter the platcfg menu. As root, run:

```
# su - platcfg
```

- b. Select Maintenance ► Upgrade ► Initiate Upgrade.
- c. Select the desired upgrade media and press Enter.

Informational messages appear on the terminal screen as the upgrade proceeds. When the 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 the post-sync healthcheck.

5. Install JRE

- a. Execute “**JRE Installation**” procedure from Appendix C in [Installation Guide](#), of the considered release

Sync Management Server with Acquisition Server

1. Set VIP

The below step should only be executed for the 1A server of the Integrated Acquisition sub-system. On Probed Acquisition standalone server the VIP is same as the IP address of the server hence no need to set the VIP.

As `cfguser` run:

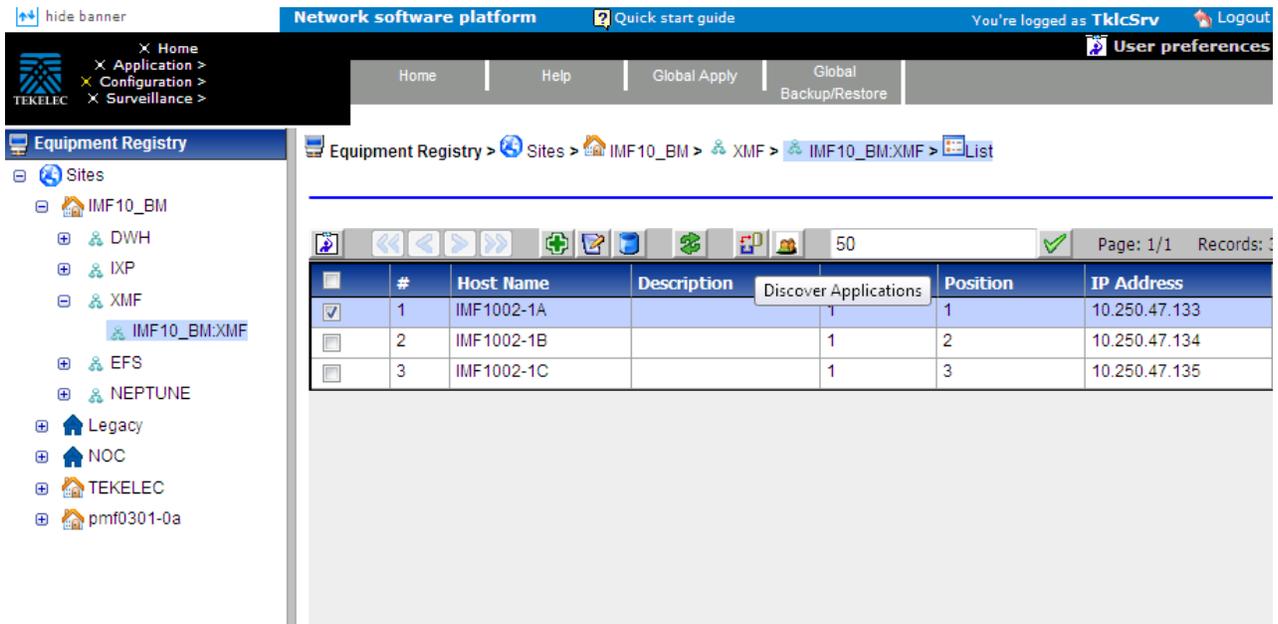
```
# setSSVIP <vip IP address>
```

2. Discover Acquisition Application on Management Server

Note: in case of DSR Monitoring, as the Acquisition server is not declared in the Centralized Configuration, move on to the next step “Sync database credentials”.

Execute the steps given below when all the servers of the sub-system are installed or if it is a standalone server

- a. From supported browser login to the NSP Application GUI as privileged user
- b. Go to the Centralized Configuration
- c. Navigate to Equipment Registry Perspective in left tree panel.
- d. Navigate to the subsystem.
- e. Select the Acquisition subsystem to synchronize by clicking on XMF under the correct Site name.
- f. This will list the subsystem in the table
- g. Select the Acquisition server and click on Discover Applications. The discover applications action should be done for each Acquisition server in the sub-system.



3. Sync Database Credentials

Execute procedure described in section **Sync Database Credentials** in [Maintenance Guide](#), of the considered release.

4. Apply Change

Note: in case of DSR Monitoring, move on to the next step “Rebuild configuration”.

- a. To Apply Changes for each subsystem go to Acquisition ► Sites ► XMF.
- b. Right click on subsystem and click on Apply Changes option on menu.

Note: If apply changes fails, then verify the accessibility of the VIP from the Management Server. If VIP address is accessible from Integrated Acquisition servers but is not accessible from Management Server, then it may be due to Cisco switch ARP table, refer to procedure **Flush ARP table** in [Hardware Guidelines](#), of the considered release.

5. Rebuild configuration

Note: these steps are to be executed in case of DSR Monitoring only.

- a. From the Centralized Configuration, take note of the Name and IP of the OCDSR, from the Equipment Registry, Sites ► <site_name> ► OCDSR
- b. Login as cfguser on the Acquisition server.
- c. Run the following command to rebuild the configuration:

```
$ webServerCLI addDsr --name=<ocdsr_name> --ip=<ocdsr_ip>
```

Note: <ocdsr_name> is the name of OCDSR and <ocdsr_ip> is its IP, both collected from the Centralized Configuration.

Acquisition Server Post-Sync Healthcheck

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

The script gathers the healthcheck information from 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 server. The output consists of a list of checks and results, and, if applicable, suggested solutions

Note: It may be possible that on login user see a message to accept or reject the upgrade, if the user has logged on to the server too soon after the reboot following upgrade. User can ignore such message as it will be cleared automatically when the startup of the server is complete.

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 refer to [Appendix A: My Oracle Support](#)

Example output for a healthy server in a sub-system:

```
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:** In case of major upgrade, the parameter must be set to New Format “2” after the Mediation server and xDR Builders have been upgraded.

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

## Chapter 7: Mediation Server Major Upgrade

This section provides the procedures for installing the Integrated xDR Platform (Mediation) application.

### Install Operating system



If the path naming feature is used Backup the files  
`/usr/TKLC/TKLCixp/prod/lib/plugins/build/SCTPPathNaming.cnf`

Refer to [Installation Guide](#) of the considered release, first to section **Mediation Guest OS reinstallation** and **Mediation Guest network** for virtual environment and to section **TPD Installation**, to install OS on the server

### Mediation Server Pre-Install Configuration

This procedure describes how to configure Mediation Server prior to installing the application.

**Note:** manufacturing must contact Project Manager or Professional Engineer in charge of the project in order to define the server hostnames in case of an extension project as this can't be changed without a complete re-installation of the software.

1. Verify each server healthcheck.
  - a. Run syscheck. Log in as root on the server that you want to install the application

As root, run:

```
syscheck
```

Review the `/var/TKLC/log/syscheck/fail_log` file for any errors. Example output of healthy server:

```
Running modules in class disk...
OK
Running modules in class proc...
OK
Running modules in class system...
OK
Running modules in class hardware...
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

**Note:** Step b and c has to be executed if error occur in this step.

- b. If the server has an external disk storage attached verify the disks state.

Check to which slot an external storage is connected. As root run:

```
hpsacli ctrl all show
```

Example output:

```
hpsacli ctrl all show
Smart Array P410i in Slot 0 (Embedded) (sn: *****)
Smart Array P411 in Slot 1 (sn: *****)
```

Now show a detailed report for each disk. As root run:

```
hpsacli ctrl slot=slot_number pd all show
```

where slot\_number is the number of the slot received in previous step. All disks must be in OK state. Example output:

```
hpsacli ctrl slot=2 pd all show
Smart Array P411 in Slot 1
array A
physicaldrive 1:0 (port 1:id 0 , Parallel SCSI, 300 GB, OK)
physicaldrive 1:1 (port 1:id 1 , Parallel SCSI, 300 GB, OK)
physicaldrive 1:2 (port 1:id 2 , Parallel SCSI, 300 GB, OK)
physicaldrive 1:3 (port 1:id 3 , Parallel SCSI, 300 GB, OK)
physicaldrive 1:4 (port 1:id 4 , Parallel SCSI, 300 GB, OK)
physicaldrive 1:5 (port 1:id 5 , Parallel SCSI, 300 GB, OK)
physicaldrive 1:8 (port 1:id 8 , Parallel SCSI, 300 GB, OK)
array B
physicaldrive 2:0 (port 2:id 0 , Parallel SCSI, 300 GB, OK)
physicaldrive 2:1 (port 2:id 1 , Parallel SCSI, 300 GB, OK)
physicaldrive 2:2 (port 2:id 2 , Parallel SCSI, 300 GB, OK)
physicaldrive 2:3 (port 2:id 3 , Parallel SCSI, 300 GB, OK)
physicaldrive 2:4 (port 2:id 4 , Parallel SCSI, 300 GB, OK)
physicaldrive 2:5 (port 2:id 5 , Parallel SCSI, 300 GB, OK)
physicaldrive 2:8 (port 2:id 8 , Parallel SCSI, 300 GB, OK)
```

- c. If the server has a SAN disk storage verify the vdisks are attached to the server.

Check to which vdisk are connected. As root run:

```
multipath -ll
```

Example of output:

```
mpathc (3600c0ff000daf12a289f0b5501000000) dm-2 HP,P2000 G3 FC
size=3.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=130 status=active
| |- 1:0:1:22 sde 8:64 active ready running
| `-- 2:0:2:22 sdi 8:128 active ready running
`-+- policy='round-robin 0' prio=10 status=enabled
|- 1:0:0:22 sdc 8:32 active ready running
`- 2:0:1:22 sdg 8:96 active ready running
mpathb (3600c0ff000daf029689c0b5501000000) dm-1 HP,P2000 G3 FC
```

```

size=3.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
| +- policy='round-robin 0' prio=130 status=active
| | - 1:0:0:21 sdb 8:16 active ready running
| | ` 2:0:1:21 sdf 8:80 active ready running
` +- policy='round-robin 0' prio=10 status=enabled
| - 1:0:1:21 sdd 8:48 active ready running
` - 2:0:2:21 sdh 8:112 active ready running

```

2. Configure the server hostname.

a. Enter the **platcfg** menu.

As root, run:

```
su - platcfg
```

b. Select **Server Configuration -> Hostname**.

c. Click **Edit**.

d. Enter the server hostname in the standard format: `ixpNNNN-MA` where:

- N is numeric 0-9
- M is numeric 1-9
- A is alphabetical a-z



**CAUTION:** be sure to reuse the same hostname as before upgrade.

**Note:** All the servers in an Mediation subsystem must have the same NNNN designation, and each server, in a subsystem, is identified by its MA designation. Always start host naming within a subsystem with “1a” as MA designation, continue with “1b”, and so on.

e. **Exit** the platcfg menu.

3. Configure the server IP.

a. For Blade servers **only**, a VLAN must be created:

As root, run:

```
su - platcfg
```

- Select Network **Configuration -> Network Interfaces**
- Click **Add an Interface**
- Select **Vlan** and press **OK**
- Set **3** as **VLAN ID**; select interface **bond0**; press **OK**
- Don't fill **MTU**; select **none** for **BootProto** and press **OK**
- Press **No** to not configure the IP address
- Exit the platcfg menu

b. Setup the IP and the default route

Refer to chapter “Manual Configuration of Ethernet Interfaces” from [Maintenance Guide](#), of the considered release.

**Note:** Use eth01 as network interface for Rack Mount servers, and bond0.3 for Blade servers.

## Install Mediation Server

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

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

**Note:** Run this procedure via iLO.

### 1. Restoring Mediation Server

- a) Log in to the Management Server Oracle machine as a root user and execute the script as below

```
/opt/nsp/scripts/oracle/cmd/restore_ixp_xmf.sh <ip_addr>
```

where ip\_addr is the ip address of the Mediation Server on which the restore is to be done.

Note: This script will ask user to provide password for *admusr* and for *root*.

- b) Once the script is successfully executed, the archive file will be restored in /var/TKLC/backup/ directory.  
**Note:** The installation procedure takes care of automatically restoring the bulkconfig in /root directory, from the archive file.
- c) On C class blade server, As root run

```
multipath -ll
```

The output of the above command should show that volume names and LUN numbers have been provided.

### 2. Log in and distribute the ISO file

- a) Open a terminal window and log in as root on the server you that you want to install the Mediation application.
- b) Distribute the media:
  - On the c-class blade server download the ISO from the PM&C ISO repository. ISOs are available on the PM&C server under the /var/TKLC/smac/image directory. Store the ISO file to /var/TKLC/upgrade directory.

### 3. Validate the installation media

- a) Enter the **platcfg menu**.

As root, run:

```
su - platcfg
```

- b) Select **Maintenance -> Upgrade -> Validate Media**.
- c) Select the desired upgrade media and press Enter.

The validation process must complete without errors. You should receive the following message:

```
CDROM is Valid
```

If any errors are reported during this validation process, then **DO NOT USE** this media to install the application.

### 4. Install the application

- a) From platcfg menu select **Maintenance -> Upgrade -> Initiate Upgrade**.  
When the installation process is complete, the server restarts automatically.

- b) 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.

5. Install JRE

- a) Execute “**JRE Installation**” procedure from Appendix C in [Installation Guide](#) of the considered release.

6. 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 A: My Oracle Support](#)

## 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:

```
$ analyze_server.sh
12:40:30: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
12:40:30: date: 08-22-11, hostname: ixp8888-1a
12:40:30: TPD VERSION: 4.2.4-70.90.0
12:40:30: IXP VERSION: [10.0.0-64.2.0]
12:40:30: XDR BUILDERS VERSION: [10.0.0-37.1.0]
12:40:30: -----
12:40:31: Analyzing server record in /etc/hosts
12:40:31: Server ixp8888-1a properly reflected in /etc/hosts file
12:40:31: Analyzing IDB state
12:40:31: IDB in START state
12:40:31: Analyzing shared memory settings
```

```
12:40:31: Shared memory set properly
.....
12:43:02: All tests passed!
12:43:02: ENDING HEALTHCHECK PROCEDURE WITH CODE 2
```

Example of a successful test:

```
12:40:31: Analyzing server record in /etc/hosts
12:40:31: Server ixp8888-1a properly reflected in /etc/hosts file
```

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, refer to [Appendix A: 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. The bulkconfig file should already be available from the restored backup.

This procedure is run from the iLO.

1. Update the bulkconfig file (if IP addresses need to be changed)
  - 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.
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
```

Note: The key exchange operation is part of this script.  
A prompt for the root and cfguser passwords appears.

      - b) Provide the appropriate passwords.
      - c) When the script is complete, check the terminal output for any errors. If the error occurs, refer to [Appendix A: My Oracle Support](#)

Note: at this step, the remote directories (used by CSV streaming feeds, for example) locally mounted before the upgrade, are automatically remounted. But, and because this is not a standard configuration, any directory (outside of PDU directories) shared by an upgraded server, is not shared again (refer to CSV streaming feeds).
  4. Generate wallet for DWS connection and Sync Database Credentials
 

Execute procedure described in section **Modify Database Password** in [Maintenance Guide](#), however user can keep the new password same as old one. The step is just needed to create DWS credentials in the wallet and sync to the mediation servers present in the sub-system.

**Note:** The above step **must** also be done for all the **Datafeeds configured** on the **OTO** server.
  5. Set VIP
 

As cfguser, run on 1A server only:

```
setSSVIP <vip IP address>
```
  6. Discover the Mediation Servers and apply configuration
    - a) Open a web browser and log in on the NSP application interface.
    - b) Open the Centralized Configuration application.
    - c) Navigate to Equipment Registry.
    - d) Open Sites and open the site; then open IXP.
    - e) Select the subsystem; select the first server and click Discover Applications in the toolbar.
    - f) Proceed as well for each server of the subsystem.
    - g) Navigate to Mediation.
    - h) Open Sites and open the site; then, open IXP.
    - i) Right-click the subsystem and select Apply changes...
    - j) Click Next and Next.
    - k) Click Apply Changes and confirm.
    - l) When change is complete, verify there is no error on the result page.

## Install xDR Builders

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

1. Associate the xDR Builders RPM with the Mediation subsystem

- a) Open a web browser and log in as TklcSrv on the NSP application interface.
  - b) Open the Upgrade Utility.
  - c) Click View Builder RPM Status in the left tree. A list of the Mediation subsystems appears.
  - d) Select one or more Mediation subsystems and click Associate RPM Package. A list of Builder RPMs that are uploaded in NSP appears.
  - e) 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 A: My Oracle Support](#)
2. 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.
3. Install the xDR Builders RPM on Mediation Server
    - a) Return to the main page of the NSP application interface.
    - 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 contact the Oracle [Appendix A: My Oracle Support](#).
4. Sessions upgrade
    - a) Click **Upgrade Session** link on left tree, this display all the sessions to be upgraded due to upgrade of associated dictionary.
    - b) Select one or more session(s) (use ctrl key for selecting multiple sessions) with **Session Upgrade Status** as either **Need Upgrade** or **Error** and choose Upgrade icon from tool bar. You may use available quick filter options on this list page to filter out sessions which you want to upgrade in one go.
 

**Caution:** Do not choose more than 5 sessions to be upgraded in one go.

Once upgrade is initiated for a session, its **Upgrade Status** will become **Upgrade Initiated**.
    - c) Once session is upgraded its **Upgrade Status** will become **Upgraded Successfully**.
5. Re-Sync the ProTraq Configurations
    - a) Open a web browser and log in to the NSP application interface tekelec user.

- b) Navigate to ProTraq Application.
  - c) Re-Sync all ProTraq Configurations by selecting each configuration and click “Synchronize and Activate Configuration” from the Configurations List Toolbar.
6. Restore the file `usr/TKLC/TKLCixp/prod/lib/plugins/build/SCTPPathNaming.cnf` from the mediation backup corresponding to individual servers in the mediation sub-system.

## 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: [10.2.0.0.0-3.2.0]
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 daemon 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 synchronizing 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  
-----

09:40:38: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0  
...  
09:41:39: All tests passed!  
09:41:39: ENDING HEALTHCHECK PROCEDURE WITH CODE 0  
END OF ANALYSIS OF SERVER ixp0907-1b

-----  
ANALYSIS OF SERVER ixp0907-1c STARTED  
-----

09:41:44: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0  
...  
09:42:40: All tests passed!  
09:42:40: ENDING HEALTHCHECK PROCEDURE WITH CODE 0  
END OF ANALYSIS OF SERVER ixp0907-1c

-----  
ANALYSIS OF SERVER ixp0907-1d STARTED  
-----

09:42:44: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0  
...

```

09:43:24: All tests passed!
09:43:25: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp0907-1d

ixp0907-1a TPD: [7.0.1.0.0-86.20.0] IXP: [10.2.0.0.0-3.2.0] XB: None
0 test(s) failed
ixp0907-1b TPD: [7.0.1.0.0-86.20.0] IXP: [10.2.0.0.0-3.2.0] XB:
[10.2.0.0.0-3.2.0] 0 test(s) failed
ixp0907-1c TPD: [7.0.1.0.0-86.20.0] IXP: [10.2.0.0.0-3.2.0] XB:
[10.2.0.0.0-3.2.0] 0 test(s) failed
ixp0907-1d TPD: [7.0.1.0.0-86.20.0] IXP: [10.2.0.0.0-3.2.0] XB:
[10.2.0.0.0-3.2.0] 0 test(s) failed

```

Example of a successful test:

```

10:24:08: Analyzing DaqServer table in IDB
10:24:08: Server ixp2222-1b reflected in DaqServer table

```

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

```

### Upgrade DTO Package

Whenever you will install or upgrade Mediation Server to a new version you need to keep DataWarehouse compatible. You need to upgrade the DTO package there. DataWarehouse is being used as an external xDR Storage.

The DataWarehouse is expected to have installed Oracle database and database instance with created login, password, data table space with name DATA\_CDR and index table space with name DATA\_IND. Such server must be already installed with DTO schema and package.

Such DataWarehouse need to be already added to management Centralized Configuration and configured.

This procedure describes how to upgrade DTO package on the DataWarehouse. This procedure doesn't describe how to install the DataWarehouse.

**Note:** If the customer refuses to provide you the SYS user password, you can provide him the files CreateDTOPkgS.sql and CreateDTOPkgB.sql to the customer DBA in order for him to proceed with the upgrade himself.

1. Check DTO package version

**Note:** Check the previous DTO package version that is installed on the DataWarehouse.

- a) Open a terminal window and log in to ActMaster server of the Mediation subsystem from which this DataWarehouse server is reachable.

As **cfguser** run:

```
$ iqt -L DatawareHouse
```

Note down Alias and Instance name of the DataWarehouse.

- b) Connect to the DataWarehouse.

As **cfguser** run:

```
$ sqlplus /@<alias>
```

Where *alias* is taken from the output in previous step.

- c) Check the DTO package version:

```
SQL> select pkg_dto.getversion from dual;
```

Quit the SQL console.

```
SQL> quit
```

## 2. Upgrade DTO package

As **cfguser** from any server of the Mediation subsystem run:

```
$ cd_oracle_utils
```

```
$ UpgradeDTOPkg.sh -a <ALIAS> <USER_NAME> <IP> <SID>
```

Or

```
$ UpgradeDTOPkg.sh <USER_NAME> <IP> <SID>
```

where:

- *ALIAS* is the Oracle DWS alias name obtained in step 1
- *IP* is the DWS IP address
- *SID* is the database instance name obtained in step 1 (Optional, default value: 'IXP')
- *USER\_NAME* is the DWH user name (optional, default value: 'IXP')

**Note:** In case `UpgradedDTOPkg.sh` is used with `"-a"` option then it will only ask password for the `"sys"` user. If the script is invoked without `"-a"` option then it will ask password for `"sys"` and DWH user name. Refer to TR006061 for the default value for the SYS password.

## 3. Verify DTO package upgrade

**Note:** Check External DataWarehouse if the DTO package has been successfully upgraded.

- a) Connect to the DataWarehouse.

As **cfguser** run:

```
$ sqlplus /@<alias>
```

Where *alias* is taken from the output received in the first step.

- b) Check the DTO package version :

```
SQL> select pkg_dto.getversion from dual;
```

Check if version of DTO package increased after upgrade. Quit the SQL console.

```
SQL> quit
```

## Mediation Server Post-Integration Configuration

This procedure describes how 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 Server 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

a) `chkconfig --levels 345 iptables off`

b) `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 8: Knowledge Base Procedures

---

### ReInstall Operating system

50 mins per server

Refer **TPD Installation** in [Installation Guide](#), of the considered release.

### Resize /var/TKLC partition

**Note:** Resize of /var/TKLC partition should be done only when required specially in case of management server where the size of ISOs is large.

Once the OS is install type the df -kh command to check the space in /var/TKLC partition.

#### Example:

```
[root@hostname1357185304]# df -kh
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root
 992M 595M 347M 64% /
/dev/mapper/vgroot-plat_tmp
 992M 34M 908M 4% /tmp
/dev/mapper/vgroot-plat_var
 992M 845M 97M 90% /var
/dev/mapper/vgroot-plat_var_tklc
 3.9G 442M 3.3G 12% /var/TKLC
/dev/mapper/vgroot-plat_usr
 3.9G 2.1G 1.7G 55% /usr
```

If space is less than 7.9 G then in order to resize /var/TKLC partition you need to be perform below mentioned steps on all servers IPM (blade and RMS) before installing applications/thirdparty product :

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

### How To Mount the ISO file from PM&C ISO Repository

This procedure describes different steps to follow to mount ISO's in PM&C repository from a blade server.

1. Add ISO in PM&C repository
  - a) Distribute the media:
    - For physical media insert the application CD/DVD into drive of PM&C server
    - For the ISO file check that iso is present under /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory. If no copy the ISO.

2. Add iso into PM&C repository
  - a) On the PM&C gui navigate to Main Menu > Software > Software Configuration > ManageSoftware Images
  - b) On the next screen choose image, put description and press Add New Image.
  - c) Wait till the adding of image is completed.

3. Record the path of the ISO
  - a) On the command line of the Management Server running PM&C, run the exportfs command to list the paths of the exported ISOs.

```
exportfs
```

- b) In the sample output below, there are 5 ISOs exported, the PM&C application, TPD, NSP package, Oracle and WebLogic You will need record the path of the ISO that you want to mount on a blade, as this path will be required in the mount command.

```
exportfs
/usr/TKLC/smac/html/TPD/PMAC--2.2.0_22.4.0--872-1818-01 169.254.102.0/24
usr/TKLC/smac/html/TPD/TPD--3.2.0_62.12.0--TPD 169.254.102.0/24
/usr/TKLC/smac/html/TPD/NSP--7.0.0-3.5.0--872-2128-101 169.254.102.0/24
/usr/TKLC/smac/html/TPD/Oracle--10.2.0.3-8--872-2115-01 169.254.102.0/24
/usr/TKLC/smac/html/TPD/Weblogic--10.3-1.2.0--872-2114-101 169.254.102.0/24
```

4. Login to blade server

Login as root user on the blade server where you want to mount the ISO

5. Start portmap service

As root run:

```
service portmap start
```

6. Start nfslock service

As root run:

```
service nfslock start
```

## 7. Create ISO mount point

As root run:

```
mkdir /mnt/local_mount_point
```

where *local\_mount\_point* is the ISO mount point on the local blade server. Example:

```
mkdir /mnt/oracle_iso
```

## 8. Mount ISO

As root run:

```
mount management_server_ip:export_path local_mount_point
```

where *management\_server\_ip* is the control network IP address of the PM&C server, *export\_path* is the export path you received in step 3 and *local\_mount\_point* is the mount point you have created in step 7. Example:

```
mount 169.254.102.4:/usr/TKLC/smac/html/TPD/oracle_10_1_0_2 /mnt/oracle_iso
```

## Adding ISO Images to the PM&C Image Repository

Refer to [Platform Configuration Guide](#), Tekelec Platform release 7.3

### How to connect a server console using iLO ssh connection

Open a ssh connection using the server iLO IP address and login with the iLO user and password

```
login as: root
root@10.31.5.100's password:
User:root logged-in to ILOUSE921N4VQ.tekelec.com(10.31.5.100)
iLO 2 Advanced 2.05 at 13:38:05 Dec 16 2010
Server Name: hostname1368545964
Server Power: On

</>hpiLO->
```

Then use the vsp command to access the server console and login with the OS user and password

```
</>hpiLO-> vsp

Starting virtual serial port.
Press 'ESC (' to return to the CLI Session.
```

```
</>hpiLO-> Virtual Serial Port active: IO=0x03F8 INT=4

CentOS release 6.3 (Final)
Kernel 2.6.32-279.5.2.el6prere16.0.1_80.32.0.x86_64 on an x86_64

hostname1368545964 login:
CentOS release 6.3 (Final)
Kernel 2.6.32-279.5.2.el6prere16.0.1_80.32.0.x86_64 on an x86_64

hostname1368545964 login:
CentOS release 6.3 (Final)
Kernel 2.6.32-279.5.2.el6prere16.0.1_80.32.0.x86_64 on an x86_64

hostname1368545964 login: root
Password:
```

## PM&C upgrade

Follow document [PM&C Incremental Upgrade](#), Tekelec Platform release 7.3

## Update the switch configurations



CAUTION: If you are working remotely you may lose the connection on the system

For **all the switches** configure the SSH access as explained in [Hardware Guide](#) doc ID E66862, of the **previous release 10.2**

For **each CISCO 3020** switch.

Configure the switch in order to add the commands from the step d

- a) As there is no log file for the following steps it is recommended to enable the log feature from your terminal in case something would not work as expected and assistance is required.
- b) Open a telnet session on the switch and then move from the user mode to privilege mode and then to config mode

```
Switch# enable
```

**Note** : for the default switch passwords refer to TR006061 (password dragon)

- c) Check the current configuration in order to see if it needs to be updated.

```
Switch# show running-config
```

- d) If some of the commands are missing go to the configuration mode and then paste the commands

```
Switch# configure terminal
```

```

link state track 1
!
interface Port-channel1
 description ISL_between_4948_and_3020
 link state group 1 upstream
!
interface range GigabitEthernet0/1-16
 description bay.ethx
 link state group 1 downstream
!
interface GigabitEthernet0/17-20
 description ISL_between_4948_and_3020
 channel-group 1 mode active

```

e) Check the configuration is modified as expected

```
Switch# show running-config
```

f) If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

g) If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

```
Switch# reload
```

## Unset Configuration on Management Server

Unset configuration application access restriction automatically set during Management Server upgrade by performing the below steps.

**Note:** Configuration application are automatically restricted to TklcSrv and tekelec user during Management Server upgrade. After required reconfiguration, Management Server shall return to normal.

1. Open a web browser and log in to the NSP application interface as TklcSrv user.
2. Navigate to security application ► Filter access
3. Select None for Restricted configuration setting.
4. Apply modification.

## Chapter 9: Management Server Backup (Post Upgrade)

---

This procedure describes how to perform a backup on a Management Server after successful upgrade.

```
ll /opt/oracle/backup/
```

Output should be:

```
drwxrwxrwx 3 oracle oinstall 4096 Apr 8 14:38 upgrade_backup
```

If the permission of /opt/oracle/backup/upgrade\_backup is not set as per above snapshot, perform the below step

```
#chmod 777 /opt/oracle/backup/upgrade_backup
```

Before proceeding with the Management Server backup, move back the backup which was copied to some other server as per steps mentioned in section 5.4

```
/opt/oracle/backup
```

As root run on mgmt. server:

```
. $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd;
sh ./launch_pic_global_backup.sh >../trc/cronNSP.log 2>&1
```

This command might take a long time depending on the size of the backup. Refer to the section “**Check Management Server Backup is valid**” of the chapter [Management Server Pre-Upgrade Healthcheck and Settings](#) in order to make sure everything went fine.

**Note:**Edit the cron job by performing the below steps.

```
#crontab -e
```

Uncomment out the launch\_pic\_global\_backup.sh entry by removing the hash(#) at the start.You might use the command crontab -l to display the list of jobs scheduled. Below should be the updated entry.

```
crontab -l
00 22 * * * . $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd;
sh ./launch_pic_global_backup.sh >../trc/cronNSP.log 2>&1
```

## Appendix A: 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.