Oracle® Communications Performance Intelligence Center

Upgrade Guide

Release 10.1

E53509 Revision 3

January 2015

Oracle Communications Performance Intelligence Center Upgrade Guide, Release 10.1

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.

See more information on MOS in the Appendix section.

Contents

1 Introduction

1.1 Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

🛑	**DANGER**: (This icon and text indicate the possibility of *personal injury*.)
⚡	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
⚠	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

1.2 Reference Documents

- Platform 6.5 Configuration Procedure Reference 909-2249-001 Revision A, December 2013
- TPD Initial Product Manufacture, 909-2130-001 Revision D, December 2013
- Platform 6.5 PM&C 5.5 Incremental Upgrade 909-2281-001, Rev A, Dec 2013
- Release Notes HP Solutions Firmware Upgrade Pack 2.2.6 , E54547 Rev 02 July 2014
- Upgrade Guide HP Solutions Firmware Upgrade Pack Release 2.2.6 E54546 Rev 02, August 2014
- PIC 10 Installation Guide E53508
- PIC 10 Maintenance Guide E53511
- Teklec Default Passwords TR006061
- PIC 10 planning guide FG005573

1.3 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*.

1.4 Scope and Audience

This document describes the major upgrade procedures for the PIC system at Release 10.

This document is intended for use by trained engineers in software upgrade on both rackmount and c-class blades system. A working-level understanding of Linux and command line interface is expected to successfully use this document.

It is strongly recommended that prior to performing an upgrade of the operating system and applications software, on a rackmount or c-class blades system, the user read through this document.

Note: The procedures in this document are not necessarily in a sequential order. There are flow diagrams in the Incremental Upgrade Overview chapter that provide the sequence of the procedures for each component of this PIC system. Each procedure describes a discrete action. It is expected that the individuals responsible for upgrading the PIC system should reference these flow diagrams during this upgrade process.

1.5 Requirements and Prerequisites

1.5.1 Hardware Requirements

For detailed information on the hardware supported refer to PIC 10 planning guide

POWER	PRODUCT	CABINET P/N	TECHNICAL REFERENCE (T.R)	SYSTEM INTERCONNECT (S.I)
G8&D2700 PRODUCT				
AC	CTRL CABINET (NSP IXP) RM	870-3115-03&04	821-0042-02	892-0098-03
AC	Extension CABINET (IXP) RM	870-3115-01&02	821-0043-02	892-0099-02
AC	PMF CABINET RM	870-3115-06&07	821-0045-02	892-0101-02
AC	BASE STORAGE C-Class	870-3115-10	821-0049-02	892-0103-11
AC	EXTENSION STORAGE C-Class	870-3115-09		892-0103-12
AC	COMPUTE C-Class	870-3115-11		892-0103-13
AC	NETWORK C-Class	870-3115-12		892-0103-14
DC	IMF DC ENTREPRISE 44U RM NEBS	870-3115-08	821-0054-02	892-0105-02
DC	IMF DC ENTREPRISE 42U RM	870-3115-05	821-0048-02	
G6&D2700 PRODUCT				
AC	CTRL CABINET (NSP IXP) RM on HP G6	870-3021-XX	821-0042-01	892-0098-XX
AC	Extension CABINET (IXP) RM on HP G6	870-3022-XX	821-0043-01	892-0099-01
AC	PMF CABINET RM on HP G6	870-3023-XX	821-0045-01	892-0101-01
AC	BASE STORAGE C-Class on HP G6 (P2000 & D2700)	870-3042-01	821-0049-01	892-0103-01
AC	EXTENSION STORAGE C-Class on HP G6 (P2000 & D2700)	870-3042-02		892-0103-02

AC	COMPUTE C-Class on HP G6 (P2000 & D2700)	870-3042-03		892-0103-03
AC	NETWORK C-Class on HP G6 (P2000 & D2700)	870-3042-04		892-0103-04
AC	LAB TRIAL C-Class on HP G6 (P2000 & D2700)	870-3042-05		892-0103-05
DC	IMF DC ENTREPRISE 36U RM on HP G6	870-3039-01	821-0046-01	892-0102-01
DC	IMF DC ENTREPRISE 42U RM on HP G6	870-3031-01	821-0048-01	892-0105-01
AC	IMF AC ENTREPRISE 42U RM on HP G6	870-3063-XX	821-0050-01	892-0107-01

1.5.2 Software Requirements

The following software is required for the PIC 10 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 PIC 9.x maintenance guide for detailed instruction.

Note: For specific versions and part numbers, see the PIC 10 Release Notice.

The following software is required for the PIC 10 installation.

Oracle Communication GBU deliverables:

- NSP
- IXP
- XDR Builder
- XMF
- TADAPT
- TPD
- TVOE
- PM&C

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

https://edelivery.oracle.com/

Other required Oracle GA deliverables can be downloaded from Oracle web site:

- WebLogic 10.3.5.0 for 64bits JVM support product Part Number V26046-01 from Oracle Fusion Middleware 11g Media Pack for Linux x86-64
    - wls1035_generic.jar

https://edelivery.oracle.com/EPD/Download/get_form?egroup_aru_number=11571971

    - jrockit-jdk1.6.0_45-R28.2.7-4.1.0-linux-x64.bin

http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-jrockit-2192437.html

Other required Oracle database patchset 13390677 deliverables can be downloaded from Oracle support site:

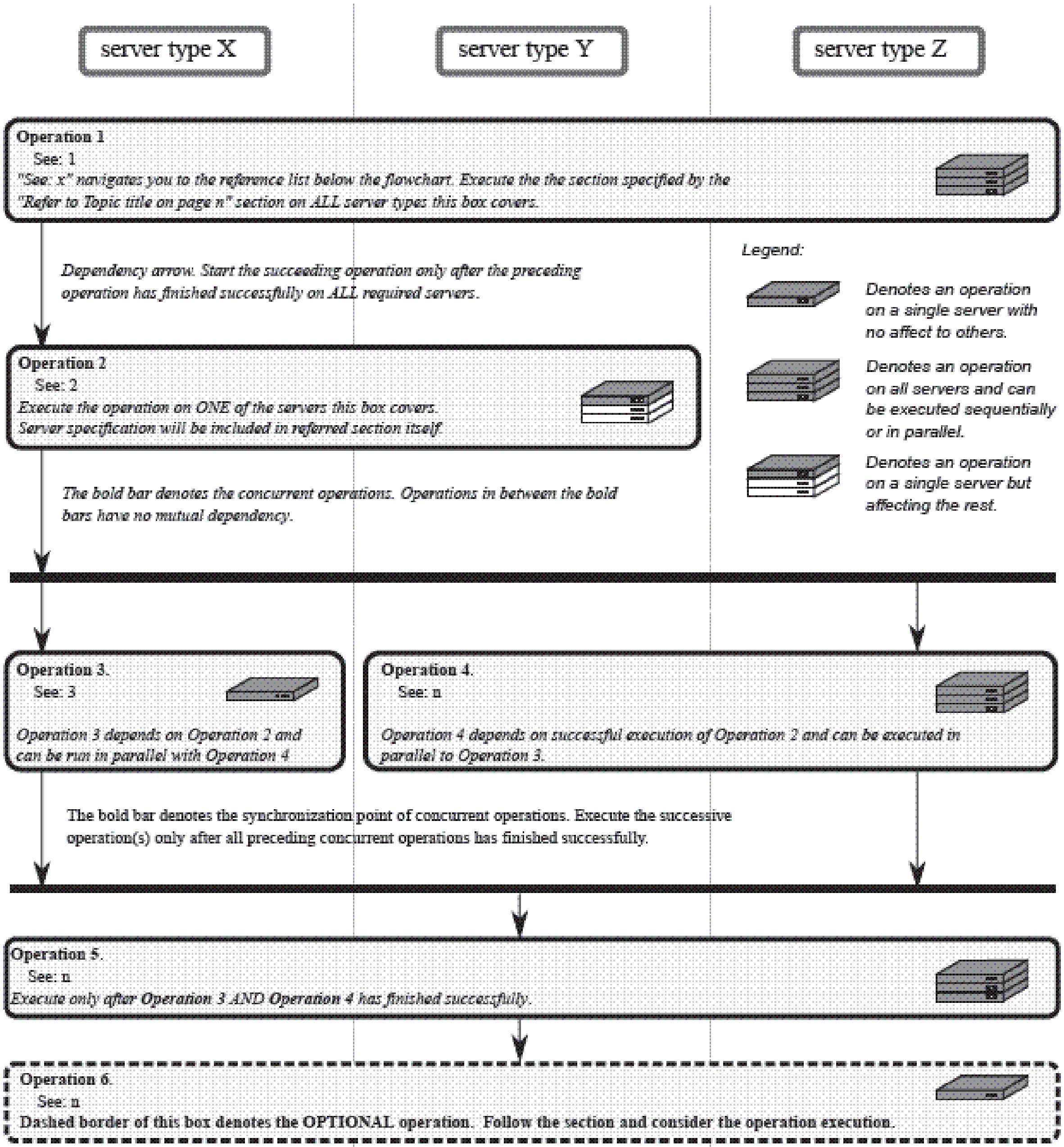
- Oracle Database 11.2.0.4 64bits product patchset
    - p13390677_112040_Linux-x86-64_1of7.zip
    - p13390677_112040_Linux-x86-64_2of7.zip
    - p13390677_112040_Linux-x86-64_3of7.zip

https://updates.oracle.com/Orion/PatchDetails/process_form?patch_num=13390677&aru=16716375&release=80112040&plat_lang=226P&patch_num_id=1730815&

2 Major Upgrade Overview Flowcharts

2.1 Flowchart Description

The flowcharts within each section depict the sequence of procedures that need to be executed to install the specified subsystem.


server type X
server type Y
server type Z
Operation 1
See: 1
"See: x" navigates you to the reference list below the flowchart. Execute the the section specified by the "Refer to Topic title on page n" section on ALL server types this box covers.
Dependency arrow. Start the succeeding operation only after the preceding operation has finished successfully on ALL required servers.
Legend:
Denotes an operation on a single server with no affect to others.
Denotes an operation on all servers and can be executed sequentially or in parallel.
Denotes an operation on a single server but affecting the rest.
Operation 2
See: 2
Execute the operation on ONE of the servers this box covers.
Server specification will be included in referred section itself.
The bold bar denotes the concurrent operations. Operations in between the bold bars have no mutual dependency.
Operation 3.
See: 3
Operation 3 depends on Operation 2 and can be run in parallel with Operation 4
Operation 4.
See: n
Operation 4 depends on successful execution of Operation 2 and can be executed in parallel to Operation 3.
The bold bar denotes the synchronization point of concurrent operations. Execute the successive operation(s) only after all preceding concurrent operations has finished successfully.
Operation 5.
See: n
Execute only after Operation 3 AND Operation 4 has finished successfully.
Operation 6.
See: n
Dashed border of this box denotes the OPTIONAL operation. Follow the section and consider the operation execution.

Each flowchart contains the equipment associated with each subsystem, and the required tasks that need to be executed on each piece of equipment. Within each task, there is a reference to a specific procedure within this manual that contains the detailed information for that procedure.

2.2 PIC High-level Major Upgrade

This flowchart describes the PIC 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.

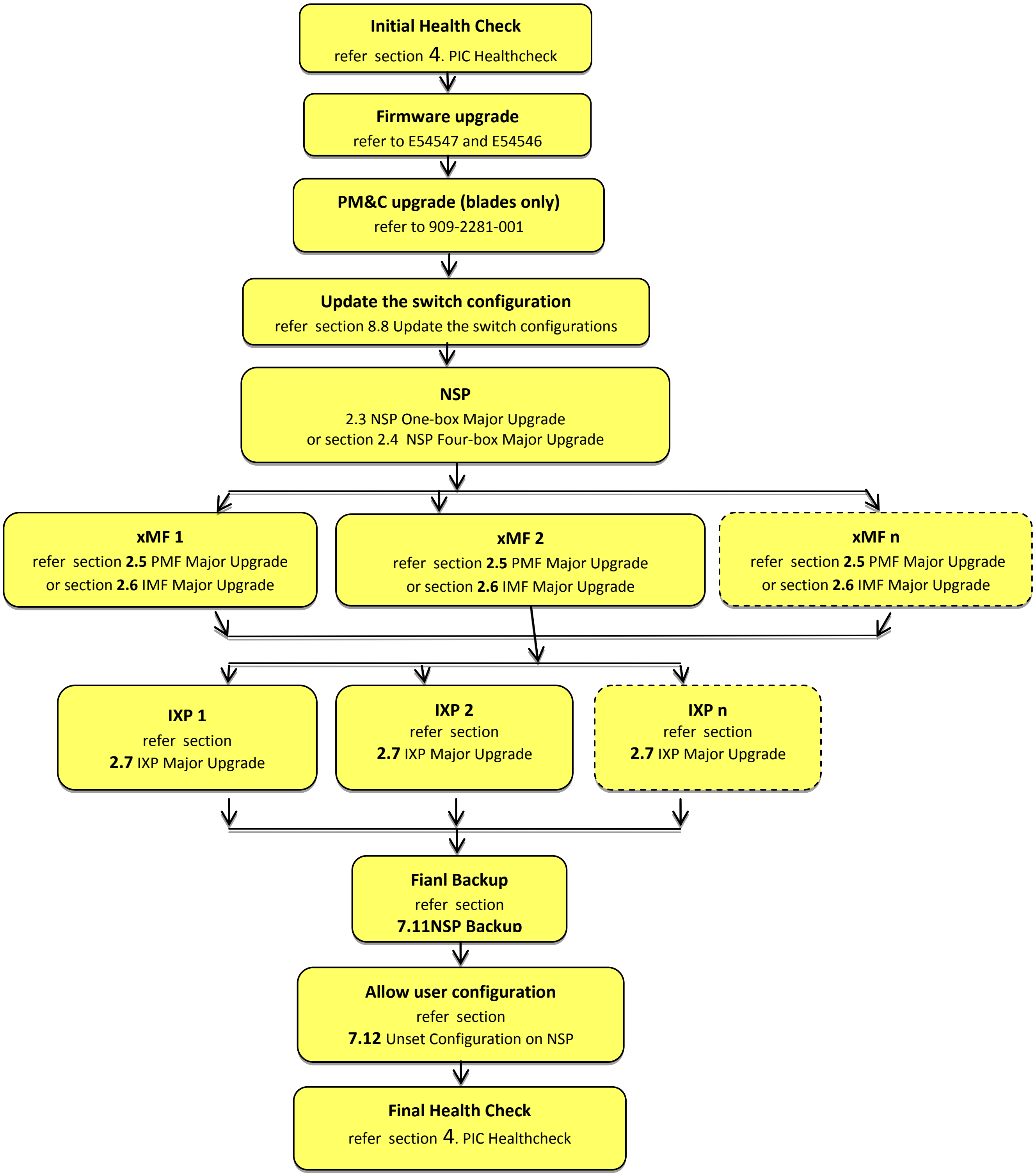
Described PIC major upgrade procedures are applicable to PIC systems installed in 9.0.3/9.0.4 releases. Following this procedure, the PIC system will be upgraded to 10 releases

Prior to starting upgrade the firmware needs to be at the latest Oracle supported levels for all hardware components. The system on the source release also need to have installed all necessary patches applicable to source release prior the major upgrade.

If running the PIC Major Upgrade on HP C-Class Blade platform the PM&C application must be upgraded first prior to PIC applications upgrade. Follow document 909-2281-001 PM&C 5.5 Incremental Upgrade for PM&C upgrade procedure.

The general upgrade strategy is as follows:

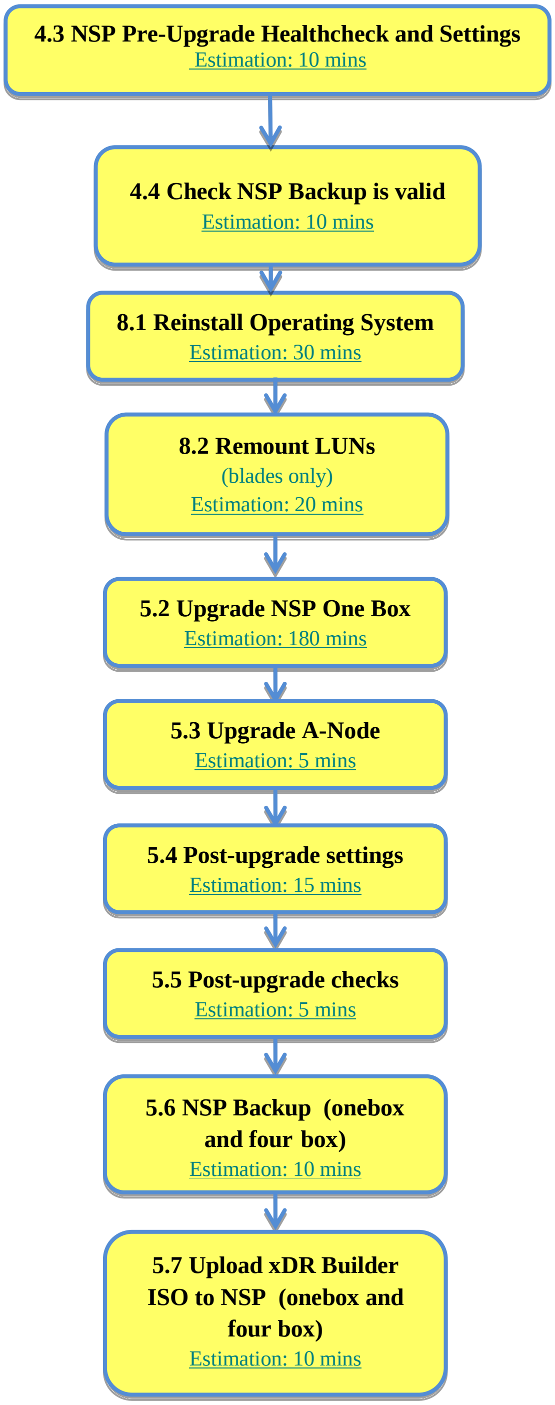
1. Initial health check at least 2 weeks before the planned operation in order to have time to replace defective hardware
2. Optional Firmware upgrade to the latest release available.
3. PM&C Platform upgrade and update the enclosure switches configuration
4. NSP upgrade (four-box or one-box configuration)
5. xMF subsystems upgrade (IMFs and PMFs)
6. IXP subsystems upgrade
7. Final Health check


Initial Health Check
refer section 4. PIC Healthcheck
Firmware upgrade
refer to E54547 and E54546
PM&C upgrade (blades only)
refer to 909-2281-001
Update the switch configuration
refer section 8.8 Update the switch configurations
NSP
2.3 NSP One-box Major Upgrade
or section 2.4 NSP Four-box Major Upgrade
xMF 1
refer section 2.5 PMF Major Upgrade
or section 2.6 IMF Major Upgrade
xMF 2
refer section 2.5 PMF Major Upgrade
or section 2.6 IMF Major Upgrade
xMF n
refer section 2.5 PMF Major Upgrade
or section 2.6 IMF Major Upgrade
IXP 1
refer section
2.7 IXP Major Upgrade
IXP 2
refer section
2.7 IXP Major Upgrade
IXP n
refer section
2.7 IXP Major Upgrade
Fianl Backup
refer section
7.11NSP Backup
Allow user configuration
refer section
7.12 Unset Configuration on NSP
Final Health Check
refer section 4. PIC Healthcheck

2.3 NSP One-box Major Upgrade

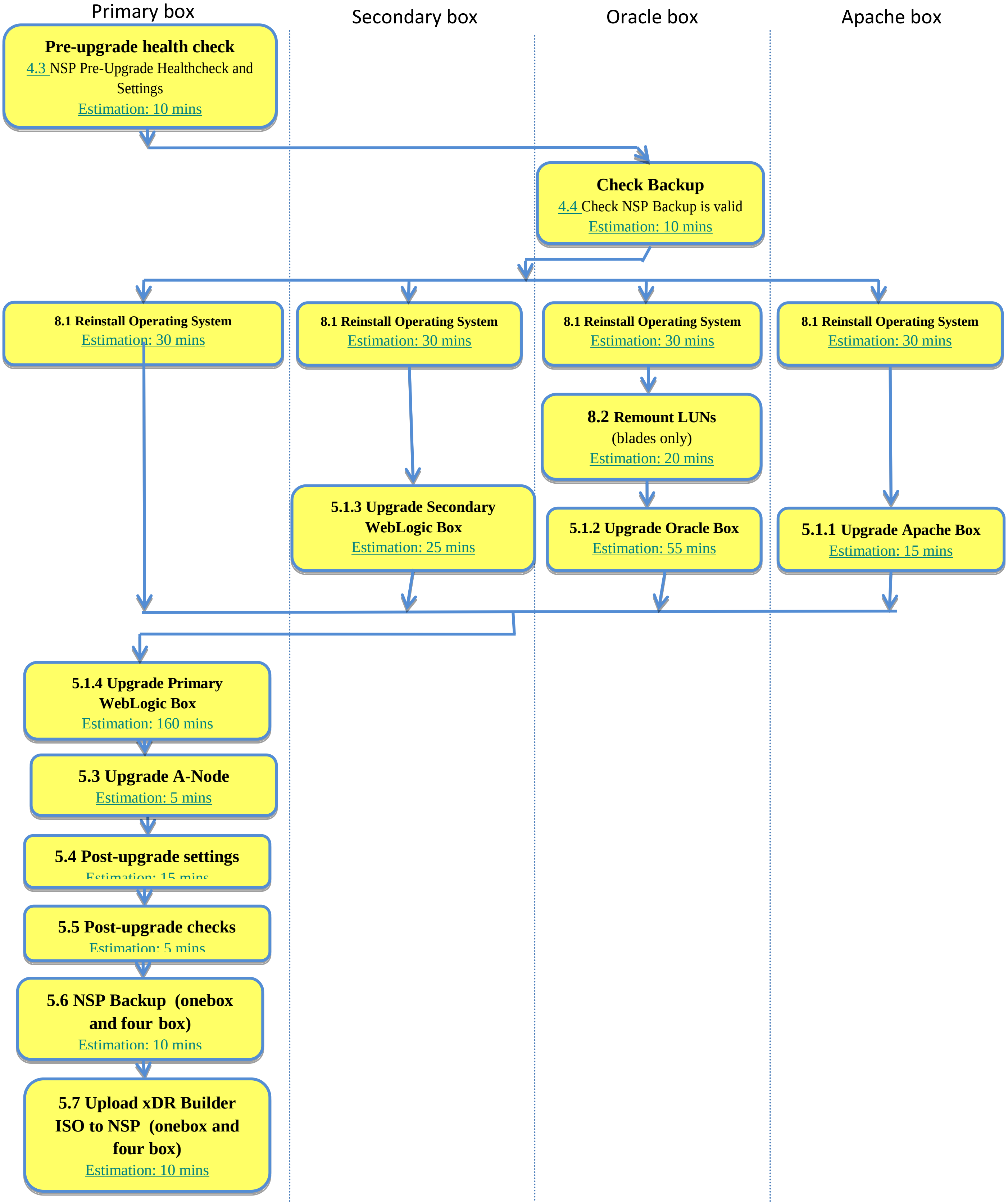
This flowchart depicts the sequence of procedures that must be executed to upgrade NSP One-box setup.

Note: On One box, time taken during upgrade of NSP product may vary depending upon the size of NSP backup



2.4 NSP Four-box Major Upgrade

This flowchart depicts the sequence of procedures that must be



executed to upgrade the NSP Four-box setup.

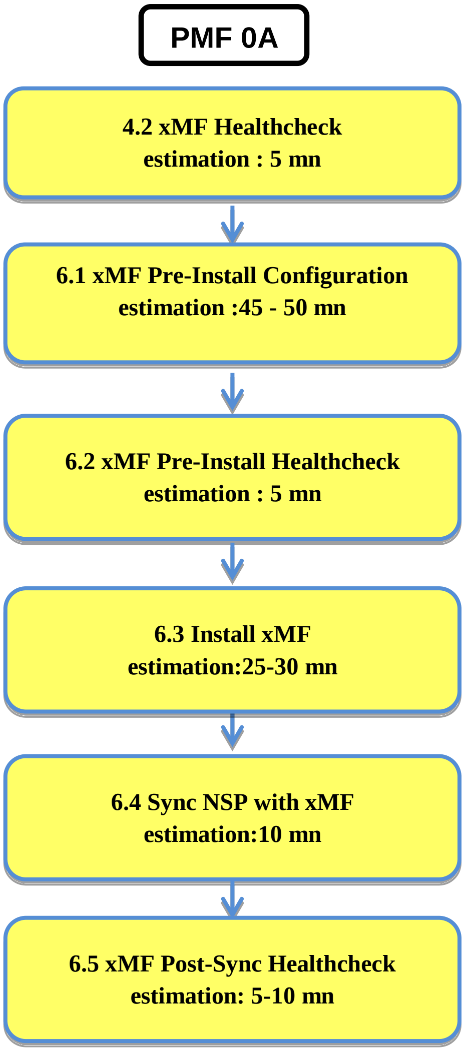
Note: On Oracle box, time taken during upgrade of NSP product may vary depending upon the size of NSP backup

2.5 PMF Major Upgrade

This flowchart depicts the sequence of procedures that must be executed to upgrade standalone PMF Server.

The procedures depicted in the flowchart pertain to standalone PMF server type.

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

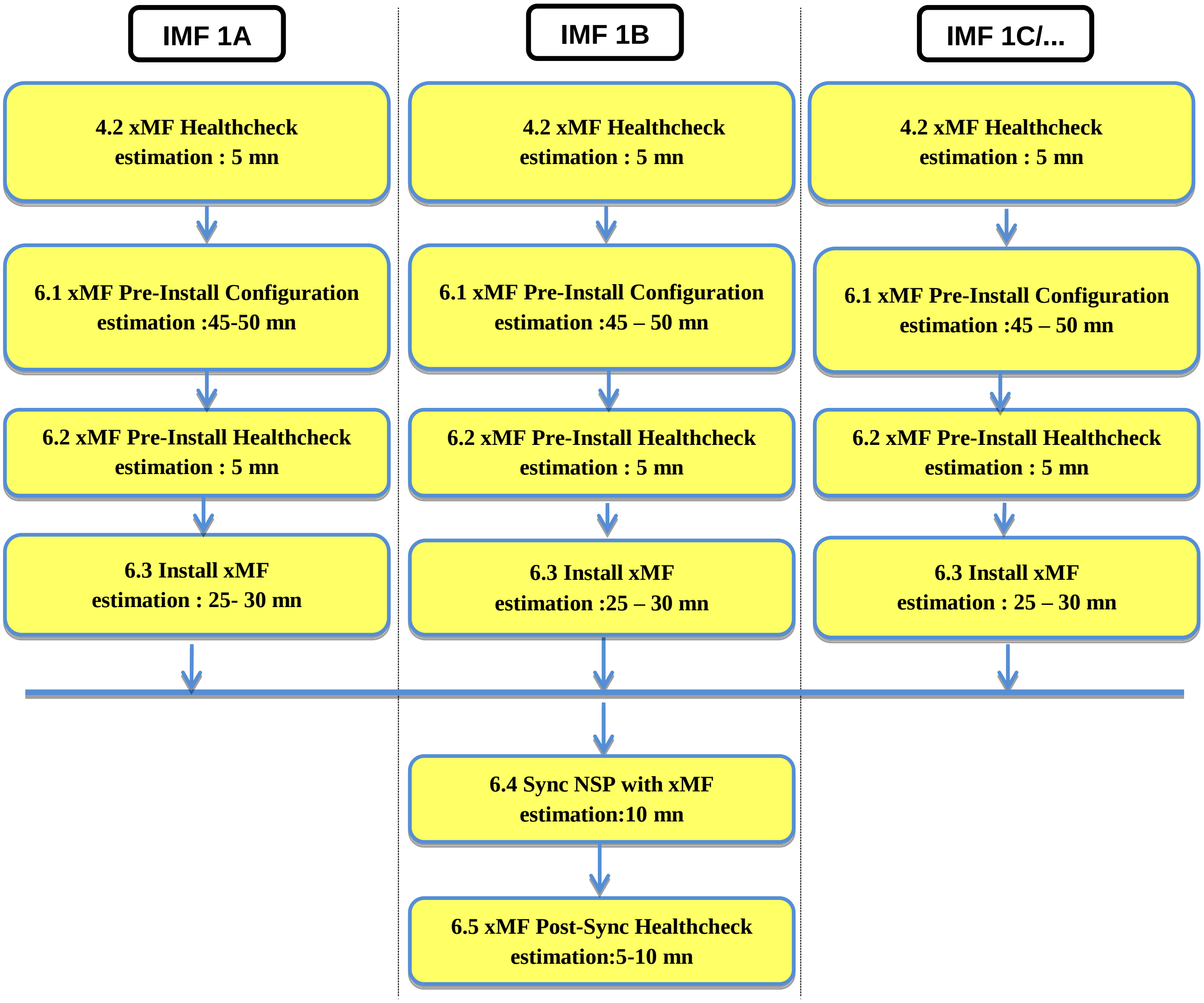


2.6 IMF Major Upgrade

This flowchart depicts the sequence of procedures that must be executed to upgrade IMF subsystem and associated servers.

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

As the servers are upgraded in parallel this procedure is introducing some data loss for the customer



2.7 IXP Major Upgrade

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

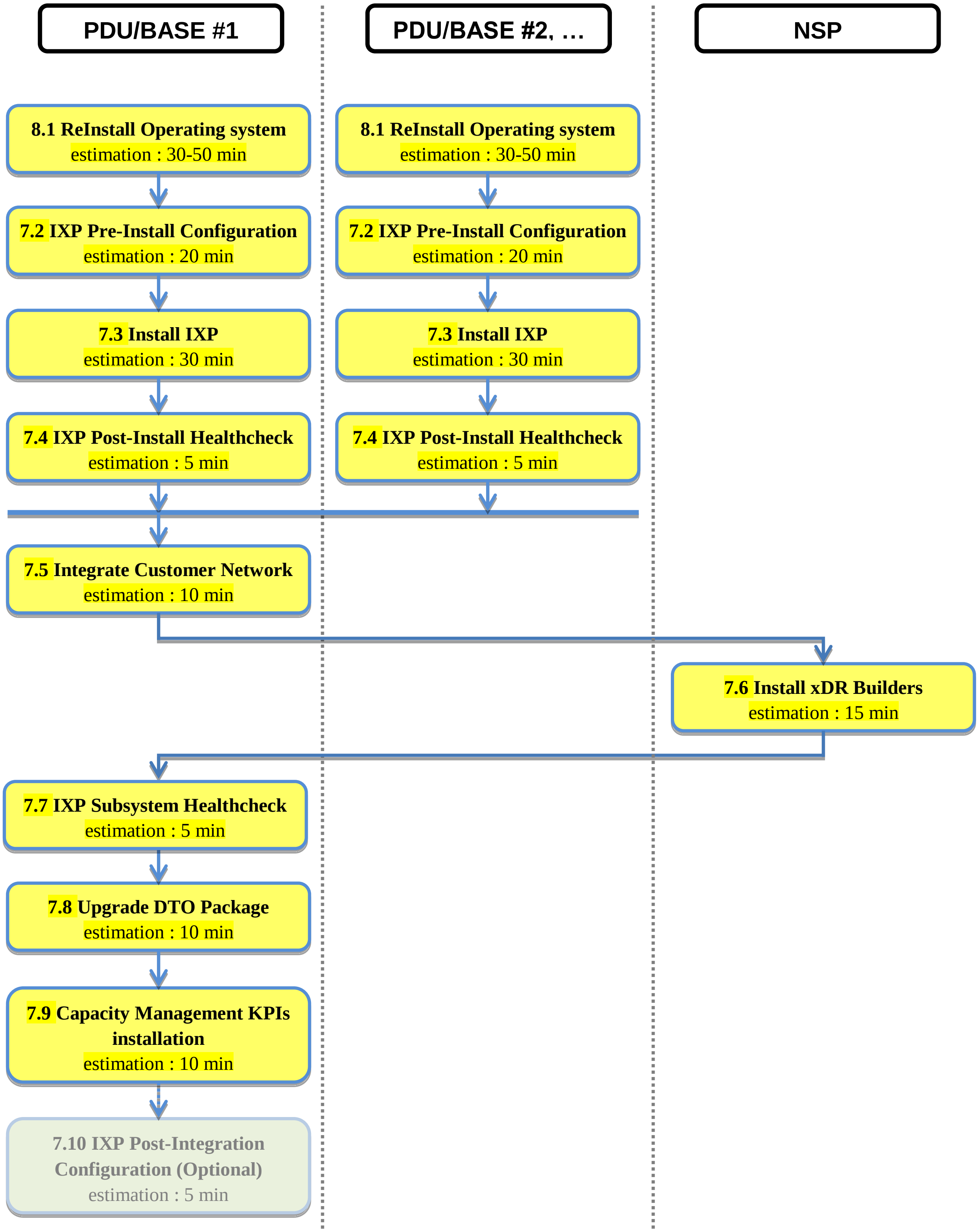
The IXP subsystem consists of the following types of servers at the beginning of the procedure:

- IXP PDU storage server
- IXP Base server

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

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 IXP subsystem, all Oracle servers where those sessions are stored must be accessible. Otherwise Centralized xDR Builder upgrade will fail.

⚠ **Note**: **xDR/DWS** server **must not be upgraded** with the new IXP software.


PDU/BASE #1
PDU/BASE #2, …
NSP
8.1 ReInstall Operating system
estimation : 30-50 min
8.1 ReInstall Operating system
estimation : 30-50 min
7.2 IXP Pre-Install Configuration
estimation : 20 min
7.2 IXP Pre-Install Configuration
estimation : 20 min
7.3 Install IXP
estimation : 30 min
7.3 Install IXP
estimation : 30 min
7.4 IXP Post-Install Healthcheck
estimation : 5 min
7.4 IXP Post-Install Healthcheck
estimation : 5 min
7.5 Integrate Customer Network
estimation : 10 min
7.6 Install xDR Builders
estimation : 15 min
7.7 IXP Subsystem Healthcheck
estimation : 5 min
7.8 Upgrade DTO Package
estimation : 10 min
7.9 Capacity Management KPIs installation
estimation : 10 min
7.10 IXP Post-Integration Configuration (Optional)
estimation : 5 min

3 Major Backout Overview Flowcharts

The **backout is** design to come back to the previous release and is applicable **only in case of successful upgrade**. The backout sequence would be similar to the upgrade sequence starting with NSP, than XMF, than IXP.
In case of issue while the upgrade you must use the Disaster recovery procedure.

3.1 NSP Major Backout

NSP application major backout is implemented as a Disaster Recovery procedure. Follow installation document of the source release to find a Disaster Recovery Procedure.
Refer to the Document 909-2247-01 PIC 9.0 Maintenance Guide.

3.2 xMF Major Backout

xMF application major backout is implemented as a Disaster Recovery procedure. Follow installation document of the source release to find a Disaster Recovery Procedure.
Refer to the Document 909-2247-01 PIC 9.0 Maintenance Guide.

3.3 IXP Major Backout

IXP application major backout is implemented as a Disaster Recovery procedure. Follow installation document of the source release to find a Disaster Recovery Procedure.
Refer to the Document 909-2247-01 PIC 9.0 Maintenance Guide

Note: Before executing section 4.12 Restore xDR Builders of 909-2247-01 guide during IXP backout process, please execute below steps too:

a) Login into NSP One-box or primary box (in case of four box) as root user and execute the below command to check if the xDR builder rpm is present.

```
# ls /var/TKLC/jmxagent/upload/
```

If the above command shows the xDR builder rpm then do not execute step b).

b) Copy the xDR builder rpm to path /var/TKLC/jmxagent/upload/ where xDR builder rpm will be the one which is mentioned in load line up.

4 PIC Healthcheck

4.1 IXP Subsystem Healthcheck

This procedure describes how to run the automatic healthcheck of the IXP subsystem, including connectity to the DWS

1. Open a terminal window and log in on any IXP server in the IXP 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
```

3. Open a terminal window and log in as cfguser on any IXP server in the IXP 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 eah 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
```

4.2 xMF Healthcheck

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

The script gathers the health check information from each server in the IMF subsystem or from PMF server. The script should be run from only on one server of the IMF 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, contact the Oracle’s Tekelec Customer Care Center.

   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!
```

2. Duplicate Suppression settings when coming from 7.1

If this feature has been configured, it is important to write down the information before starting the upgrade and to add them again in the CCM after the upgrade

For this:

- igrep -p DupIpPktTimeoutMs LongParam
- iqt -pz -f_name -f_dupIpPktEnabled DbIpLink

3. Check in the CCM if the PMF is using an expert mode file. Navigate to Acquisition > Sites > Site Name > PMF name > Servers > PMF Name > PMIA Configurations and check if a file is active. In this case this file superceed whatever is configured in the CCM, but requires to keep the same TC id used. That's why you need to ensure it remain the same using the following command as cfguser

```
PMF1-0A:/export/home/cfguser iqt -p DbIpLink
 id  filterId  policy  applicationType  filterType  mfGroupId  pduTblId  name
 shortName  msgFeederId  protocol  preFilter  advFilter  ipSessTimeout
 ipSessForcedTimeout  ipSessTruncation  ipSessFwdCnt  ipSessCntInterim
 ipSessDirection  dupIpPktEnabled  lastTime
16932 0 -1 GENERIC PKT PMF1:XMF 0 PMF1-0A All 16932 PMF1-0A 127  ( port 2152
or port 3386 or port 2123) 0 864000 0 No 0 SESSION WAY BOTH No 11/19/2012
15:23:29
```

4.3 NSP Pre-Upgrade Healthcheck and Settings

This procedure describes pre-upgrade sanity test NSP together with a few configuration settings. The main goal is to have a backup using the **PIC 10 script** however the server is not yet upgraded.

1. Removal of report server platform

a) Report server platform is not supported from 10 release, so before upgrading make sure it is removed from the PIC system if present.

Note: For removing a Report Server, please refer the installed analytics packages user manuals for deletion of configuration and for uninstallation of the installed analytics packages. After that delete the RSP subsystem from CCM application on NSP.

Do not proceed to the following steps if RSP is still installed, otherway it will be part of the configuration upgraded.

2. Copy NSP ISO file

a) Log in as root on the NSP server (In case of Onebox configuration) or all Four Boxes (In case of Four Box Configuration) and copy the **NSP 10** iso to /var/TKLC/upgrade folder.

b) On the c-class blade server download the **NSP 10** 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. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure Adding ISO Images to the PM&C Image Repository

3. Mount the media

As `root`, run the appropriate command to mount the media:

```
# mount –o loop iso_path /mnt/upgrade
```

where iso_path is the absolute path of the NSP ISO image, which includes the name of the image (starting with /var/TKLC/upgrade).

4. PIC backup

Note: The backup must be done with the backup script available in 10 ISO.

a) Log in as `root` on the NSP server (In case of Onebox configuration) or all the Four Boxes (In case of Fourbox configuration)

b) On Onebox server or FourBox server (all boxes), perform the below steps
   i. cp /opt/nsp/scripts/oracle/cmd/LaunchExpNSP.sh /opt/nsp/scripts/oracle/cmd/LaunchExpNSP.sh_bkp
   ii. cp /opt/nsp/scripts/oracle/cmd/ExeCheck.sh /opt/nsp/scripts/oracle/cmd/ExeCheck.sh_bkp
   iii. cp /opt/nsp/scripts/ExpNSPSys.sh /opt/nsp/scripts/ExpNSPSys.sh_bkp

c) On Onebox server or FourBox server (all boxes), perform the below steps
   i. scp **/**mnt/upgrade/scripts/{**launch_pic_global_backup.sh,pic_global_backup.sh,ixp_xmf_backup.sh,LaunchExpNSP.sh**,ExeCheck.sh,**ixp_backup.sh,xmf_backup.sh**} /opt/nsp/scripts/oracle/cmd/
   ii. scp /mnt/upgrade/scripts/ExpNSPSys.sh /opt/nsp/scripts/ExpNSPSys.sh
   Note: In case user is prompted for message as below, please press 'y' to continue
   scp: overwrite '/opt/nsp/scripts/ExpNSPSys.sh'?

As root user, change permission of all the files as per below:

Onebox server or Four Box server (all boxes):

i. chmod 777 /opt/nsp/scripts/oracle/cmd/*
ii. chmod 777 /opt/nsp/scripts/ExpNSPSys.sh

d) On One Box server or Primary Box server, go to the path /opt/nsp/scripts/oracle/cmd and do the below step

```
# crontab –e
```

Change LaunchExpNSPdp.sh to launch_pic_global_backup.sh if present

and save the changes

This should be the updated entry

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

e) On One Box server or Primary Box server, go to the path /opt/nsp/scripts/oracle/cmd and run the below script.

```
# sh launch_pic_global_backup.sh
```

The above script will take the NSP backup on one box server or oracle box server along with the IXP/xMF 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!

4.4 Check NSP Backup is valid

This procedure describes different steps to be followed for checking the backup of NSP 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. This must be verified on One Box server or Oracle Box server.

```
# 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 NSP backup is on external drives or not.
   i. Login as root on NSP one box or oracle box in case of 4 box system and execute below commands.

```
# cd /opt/oracle/backup
# df -h .
Filesystem                  Size  Used Avail Use% Mounted on
/dev/mapper/nsp_backup_vol  138G  2.1G  136G   2% /usr/TKLC/oracle/backup
```

In case of Blade system output will be like as above.

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

In case of RMS system output will be like as above.

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 contact Oracle Customer Care Center.

b) Check the content of the last backup directory

For a One Box

```
-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
-rw-r--r--  1 root   root       116 Mar 24 22:01 bulkconfig
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 **IXP** 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
```

Check the content of **XMF** backup folder

```
-rw-r--r-- 1 root   root      296 Mar 24 22:01 XMF_xmf-9010.tgz
```

For a Four Box

```
# cd NSP BACKUP 07 04 12 22 00 01
# ls -lh
total 60K
drwxr-xr-x  2 root root 4.0K Jun  8 22:01 apache
-rw-r--r--  1 root root 3.0K Jun  8 22:01 backup.log
-rw-r--r--  1 root root  186 Jun  8 22:00 boot.properties
drwxr-xr-x 10 root root 4.0K Jun  8 22:00 config
drwxrwxrwx  2 root root 4.0K Jun  8 22:00 exportrealm
```

```
-rw-r--r--  1 root root    0 Jun  8 22:01 failedconnection.txt
-rw-r--r--  1 root root 2.5K Jun  8 22:01 global_versions.properties
-rw-r--r--  1 root root  486 Jun  8 22:01 hosts.csv
drwxrwxrwx  2 root root 4.0K Jun  8 22:01 IXP
drwxr-xr-x  7 root root 4.0K Jun  8 22:00 ldap
drwxrwxrwx  2 root root 4.0K Jun  8 22:01 oracle
-rw-r--r--  1 root root  320 Jun  8 22:00 preBackupTests.log
drwxr-xr-x  2 root root 4.0K Jun  8 22:01 primary
drwxr-xr-x  2 root root 4.0K Jun  8 22:01 secondary
-rw-r--r--  1 root root   64 Jun  8 22:00 SerializedSystemIni.dat
drwxrwxrwx  2 root root 4.0K Jun  8 22:01 XMF
```

Check the content of the oracle directory and 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`

```
# ls -lh oracle/
total 87M
-rw-r--r-- 1 root   root      448 Jun  8 22:01 bulkconfig
-rw-r--r-- 1 oracle oinstall  37M Jun  8 22:01 ExpNSP.dmp.gz
-rw-r--r-- 1 oracle oinstall  52K Jun  8 22:01 ExpNSP.log
-rw-r--r-- 1 root   root     2.5K Jun  8 22:01 global_versions.properties
-rw-r--r-- 1 root   root      203 Jun  8 22:01 hosts
-rw-r--r-- 1 root   root      152 Jun  8 22:01 ifcfg-bond0.3
-rw-r--r-- 1 root   root       76 Jun  8 22:01 ifcfg-eth02
-rw-r--r-- 1 root   root      47K Jun  8 22:01 install.log
-rw-r--r-- 1 root   root      50M Jun  8 22:01 jmxagentproperties.tgz
-rw-r--r-- 1 root   root       88 Jun  8 22:01 network
-rw-r--r-- 1 root   root       63 Jun  8 22:01 nsp setenv.sh
-rw-r--r-- 1 root   root     1.8K Jun  8 22:01 ntp.conf
-rw------- 1 root   root     2.8K Jun  8 22:01 snmpd.conf
```

c) Verify that bulkconfig file and global_version.properties file must be present in the latest backup directory in case of One Box server. In case of Four Box Configuration, on Oracle Box, verify that bulkconfig file is present inside primary, secondary, apache and oracle folder inside latest backup directory and global_version.properties file inside the latest backup directory.

d) ExpNSP.dmp.gz file should not be empty.

e) In exportrealm directory four files i.e. `DefaultAuthenticator.dat`, `DefaultCredentialMapper.dat`, `XACMLAuthorizer.dat`, `XACMLRoleMapper.dat` should be present

f) On One Box server or Oracle Box server, run healthcheck:

- For the ISO file, run:

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

Example (one box):

```
[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/exportrealm/DefaultAuthenticator.dat
File exists [ OK ].
/opt/oracle/backup/NSP BACKUP 03 30 14 22 00 01/exportrealm/DefaultCredentialMapper.dat
File exists [ OK ].
/opt/oracle/backup/NSP BACKUP 03 30 14 22 00 01/exportrealm/XACMLAuthorizer.dat File
exists [ OK ].
/opt/oracle/backup/NSP BACKUP 03 30 14 22 00 01/exportrealm/XACMLRoleMapper.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.

g) Copy backup directory

i. Login as a root user on NSP Server (In case of Onebox configuration) or Oracle server (In case of fourbox configuration).

ii. Verify the NSP 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 -dtr /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 contact Oracle Customer Care Center.

iii. Verify the size of NSP 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 previos step, using below command

```
# scp -r /opt/oracle/backup/NSP BACKUP XX XX XX XX XX XX <Server
IP>/<Directory_Path>
```

4.5 Disable the cron job which takes PIC backup (four box only)

Once the backup and its health check is complete, edit the cronjob by performing the below steps. This will ensure that no intermediate PIC backup is created during Major upgrade cycle.

a) Login as a root user on NSP Primary server and do the below step:

```
# 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
01 00 * * *  rm -rf /tekelec/backup`date \+\%u`;/usr/TKLC/TKLCmf/bin/backup config
backup`date \+\%u` > /tekelec/TKLCmf/runtime/run/log/backup`date \+\%u`.log
```

4.6 Upgrade build DFP using builders no more supported

Before doing an upgrade, all build DFP should be checked in CCM.

And if some of them are still using following builders they should be updated by removing those EOL builders :

- GPRS Gb Stats
- IMS COPS TDR
- IP i-mode TDR
- SS7 IS-41 DB TDR
- SS7 MAP DB TDR
- SS7 CAMEL DB TDR
- SS7 ISUP ANSI Sentinel CDR
- SS7 SMDR
- Traffic Classification Stats
- UMTS IuC Control SUDR
- UMTS IuC RAB TDR
- UMTS IuP Control SUDR
- UMTS IuP RAB TDR
- VoIP GSX SONUS CDR
- IP BGP Stats
- IP Basic TDR
- IP IUA SUDR
- VoIP MGCP CEGETEL CDR

4.7 Upgrade Configurations using Deprecated Field(s)

This step is to be performed to upgrade configurations which are using Deprecated field(s) so as to make sure none of the configuration will use Deprecated field which may get removed in later releases.

a) Login to NSP application interface as TklcSrv user.

b) Click **Upgrade Utility**

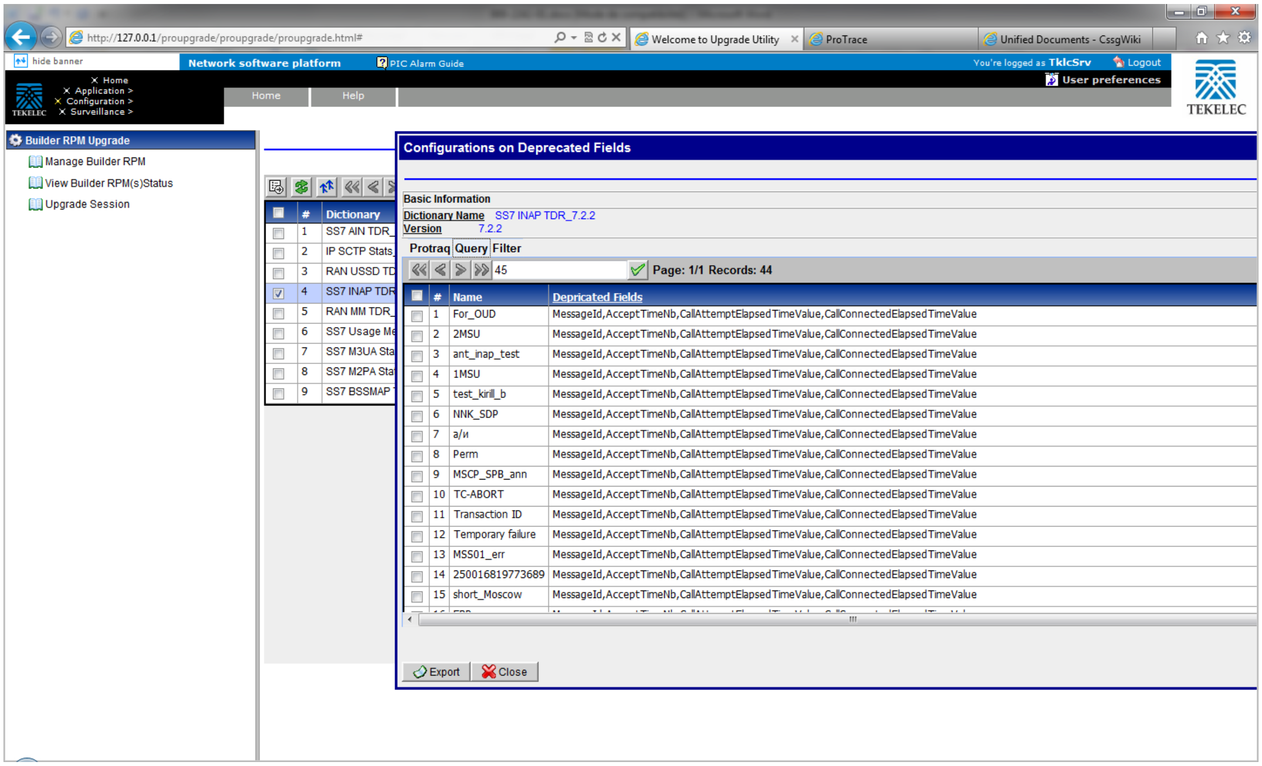
c) Click **Dictionaries with Deprecated Field(s)** link on home page, this will a list of dictionaries having deprecated field(s).

d) Select any one of the dictionaries and choose **View Dependant Configurations** icon from tool bar.

This will display list of Protraqs, Queries and Filters using deprecated fields. You can also export this list by clicking on **Export** button given on that popup. If there are no dependant configurations then this list will be empty.

WARNING

warning: Take care to check each Tab and not Only the default one ProTraq. The Screen shot bellow shows an example where the job has not been done at the end of the previous upgrade.



	#	Dictionary
□	1	SS7 AIN TDR_
□	2	IP SCTP Stats_
□	3	RAN USSD TD
☑	4	SS7 INAP TDR
□	5	RAN MM TDR_
□	6	SS7 Usage Me
□	7	SS7 M3UA Sta
□	8	SS7 M2PA Sta
□	9	SS7 BSSMAP

Configurations on Deprecated Fields

Basic Information

Dictionary Name SS7 INAP TDR_7.2.2

Version 7.2.2

Protraq Query Filter

45 Page: 1/1 Records: 44

□	#	Name	Depricated Fields
□	1	For_OUD	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	2	2MSU	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	3	ant_inap_test	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	4	1MSU	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	5	test_kirill_b	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	6	NNK_SDP	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	7	а/и	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	8	Perm	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	9	MSCP_SPB_ann	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	10	TC-ABORT	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	11	Transaction ID	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	12	Temporary failure	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	13	MSS01_err	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	14	250016819773689	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue
□	15	short_Moscow	MessageId,AcceptTimeNb,CallAttemptElapsedTimeValue,CallConnectedElapsedTimeValue

WARNING

warning: The fields deprecated in 7.x release will be removed in the release 10 dictionaries. Their related configurations (like Queries, Filters and Protraqs) will be deleted during the protocol upgrade procedure. Make sure such configurations are upgraded to the latest dictionaries as mentioned in section 5.7 Upload xDR Builder

ISO to NSP (onebox and four box). These deprecated fields will be removed from the sessions by the nightly jobs on the DWS.

4.8 Global Healthcheck

4.8.1 iLO Access

CAUTION: Make sure you can access the iLO interface of all servers and you can open the remote console for each server. Starting PIC 10 software **installation through SSH is blocked** and it can be done only on the server console it self or unsing iLO.

4.8.2 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.

4.8.3 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

Note: For blade system make sure all the LUN information are documented and you will not be blocked when you will need to remount the NSP SAN volumes

4.8.4 ProTrace Session Status

Navigate from the home screen to ProTrace

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

1. View All records
2. Filter by end date
3. End date must be the correct time
4. 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.

4.8.5 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.

4.8.6 Alarm Forwarding

Connect on NSP Primary 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.

4.8.7 ProTraq

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

4.8.8 ProPerf

Access to ProPerf configuration and check each dashboard is working fine

4.8.9 DataFeed

Access to the DataFeed configuration and capture the Feed Status
Make sure each Feed configuration is Documented in the Engineering Document

4.8.10 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.

4.8.11 Diagnostic Utility

Pre-upgrade healthcheck should be done using the diagnostic utiity.
Access to Diagnostic utility and navigate to each system to make sure the system is healthy.

If the healthcheck is done post major upgrade then instead of diagnostic utility capacity management feature should be used.
Access ProTrace and open PIC_UsageStats session to verify if normal activity is monitored hourly for probed acquisition, integrated acquisition, mediation and mediation protocol.

5 NSP Major Upgrade

This section provides the procedures for upgrading the NSP application

5.1 Upgrade Four Box setup

Follow the below mentioned steps to upgrade four box setup:

Warning: This step is applicable to four box configuration only. Skip it for onebox config

5.1.1 Apache Box

If not already done refer *ReInstall Operating system* **to reinstall the machine.**

1) Log in as **root** on the server. As root user run:
   `#` **`syscheck`**
   Review the `fail_log` file `(/var/TKLC/log/syscheck/fail_log)` for any errors .

Example ouput for a healthy system:

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

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

2) **Configure the server hostname**

   a) As `root`, run:

   `#` **su - platcfg**

   b) Select **Server Configuration ➢ Hostname** .

   c) Click **Edit.**

   d) Type the NSP Apache server hostname and click **OK**.

   e) Return to the main **platcfg** menu.

3) **Configure SNMP**

   a) From the main **platcfg** menu, select **Network Configuration➢SNMP Configuration➢NMS Configuration** and select **Edit > Add A New NMS Server**.

   b) Type the IP address as **127.0.0.1** and **TEKELEC** as the community string and port number is not optional (port number 162) and then click **OK** and then **EXIT**

   c) Click **YES** to restart alarm server and then press any Key to continue.

   d) Exit the **platcfg** menu.

4) **Temporary customer IP assignement**
   Refer section 4.1.5 Temporary customer IP assignment in E53508-01.docx

5) **Copy NSP ISO**

   a) Copy NSP iso to /var/TKLC/upgrade folder.

   b) 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/repository directory. Store the ISO file to /var/TKLC/upgrade directory. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure Adding ISO Images to the PM&C Image Repository

6) **Mount ISO**

As root, run:

```
# mount -o loop iso_path /mnt/upgrade
```

where iso_path is the absolute path of the NSP ISO image, which includes the name of the image (starting with /var/TKLC/upgrade).

7) **Copy bulkconfig**

a) Copy the bulkconfig file from backup directory(from the server on which you have copied during pre health check steps) to /root directory.

8) **Upgrade Apache Box**

a) Login as root user on the Apache Box.

b) As `root`, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
# /mnt/upgrade/upgrade_nsp.sh
Where /mnt/upgrade is the mount point where NSP iso is mounted
```

c) Wait for NSP installation to get complete. 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.

d) After the installation the server will restarts automatically. Log back in and review the NSP installation log (/var/log/nsp/install/nsp_install.log) and TPD upgrade log (/var/TKLC/log/upgrade/upgrade.log) for errors.

If NSP did not install successfully, contact the Oracle Customer Care Center.

Note: When user will login back to machine then a message will appear asking to accept or reject upgrade. Ignore this message for now. It will be automatically accepted when user will execute `post_upgrade_sanity_check.sh script during` *NSP Post-Upgrade Check (onebox and four box).*

5.1.2 Oracle Box

If not already done refer *ReInstall Operating system* **to reinstall the machine and** *Remount NSP LUN(C-class blades only)* **for blade server only**.

1) Login as root user and run:

```
# syscheck
```

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

Example ouput for a healthy system:

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

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

2) **Configure the server hostname**

a) As `root`, run:

```
# su - platcfg
```

b) Select **Server Configuration ➤ Hostname** .

c) Click **Edit.**

d) Type the NSP Oracle server hostname and click **OK**.

e) Return to the main **platcfg** menu.

3) **Configure SNMP**

a) From the main **platcfg** menu, select **Network Configuration➤SNMP Configuration➤NMS Configuration** and select **Edit > Add A New NMS Server**.

b) Type the IP address as **127.0.0.1** and **TEKELEC** as the community string and port number is not optional (port number 162) and then click **OK** and than **EXIT**

c) Click **YES** to restart alarm server and then press any Key to continue.

d) Exit the **platcfg** menu.

4) **Temporary customer IP assignement**

Refer section 4.1.5 Temporary customer IP assignment in E53508-01.docx

5) **Copy NSP ISO**

a) Copy NSP iso to /var/TKLC/upgrade folder.

b) 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/repository directory. Store the ISO

file to /var/TKLC/upgrade directory. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure Adding ISO Images to the PM&C Image Repository

c) Download the following files from Oracle Download center and copy them to /var/TKLC/upgrade folder:

- For Oracle Database 11.2.0.4 product
  - p13390677_112040_Linux-x86-64_1of7.zip
  - p13390677_112040_Linux-x86-64_2of7.zip

6) **Mount NSP ISO**

As root, run:

```
# mount -o loop iso_path /mnt/upgrade
```

where iso_path is the absolute path of the NSP ISO image, which includes the name of the image (starting with /var/TKLC/upgrade).

7) **Copy bulkconfig**

a) Login as root user on the Apache Box.
b) Copy the bulkconfig file from Apache box to /root directory.

8) **Upgrade Oracle Product**

a) Login as root user on the Oracle Box.

b) As `root`, run:

Note: Run this procedure via iLO or through any non disconnectable console only

```
       # /mnt/upgrade/install_oracle.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted.
```

c) System will reboot after successful installation of oracle

d) Review the installation log (/var/TKLC/log/upgrade/oracle.log) for any errors. Oracle must be installed successfully.

If there are any errors, contact the Oracle PIC Design Support Team

9) **Verify NSP Backup**

a) Login as root user on the Oracle Box.

b) Verify the NSP backup on which the healthcheck was performed using "section 4.4 Check NSP Backup is valid " is present and is the latest backup. Execute the below command to find out the latest backup directory:

```
# ls -dtr /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 with upgrade and contact Oracle Customer Care Center.

10) **Upgrade NSP**

a) Log in as root on the server to install the NSP application.

b) For an NSP ISO file copied in /var/TKLC/upgrade run:

```
# mount –o loop iso_path /mnt/upgrade
```

where iso_path is the absolute path of the NSP ISO image, which includes the name of the image (for example, /var/TKLC/upgrade/iso_file_name.iso).

- 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/repository directory. Store the ISO file to /var/TKLC/upgrade directory. If the ISO is not present in PM&C ISO repository.

c) As `root`, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
# /mnt/upgrade/upgrade_nsp.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted
```

d) Wait for NSP installation to get complete. 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.

e) After the installation the server will restarts automatically. Log back in and review the NSP installation log (/var/log/nsp/install/nsp_install.log) and TPD upgrade log (/var/TKLC/log/upgrade/upgrade.log) for errors.

If NSP did not install successfully, contact the Oracle Customer Care Center.

Note: When user will login back to machine then a message will appear asking to accept or reject upgrade. Ignore this message for now. It will be automatically accepted when user will execute `post_upgrade_sanity_check.sh script during` *NSP Post-Upgrade Check (onebox and four box)*

5.1.3 Secondary WebLogic Box

If not already done refer *ReInstall Operating system* to reinstall the machine

1) **Login as root user and run**:

```
# syscheck
```

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

Example ouput for a healthy system:

```
Running modules in class disk...
```

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

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

2) **Configure the server hostname**

a) As `root`, run:

`#` **su - platcfg**

b) Select **Server Configuration ➢ Hostname** .

c) Click **Edit.**

d) Type the NSP WebLogic Secondary server hostname and click **OK**.

e) Return to the main **platcfg** menu.

3) **Configure SNMP**

a) From the main **platcfg** menu, select **Network Configuration➢SNMP Configuration➢NMS Configuration** and select **Edit > Add A New NMS Server**.

b) Type the IP address as **127.0.0.1** and **TEKELEC** as the community string and port number is not optional (port number 162) and then click **OK** and than **EXIT**

c) Click **YES** to restart alarm server and then press any Key to continue.

d) Exit the **platcfg** menu.

4) **Temporary customer IP assignement**

Refer section 4.1.5 Temporary customer IP assignment in E53508-01.docx

5) **Copy NSP ISO**

a) Copy NSP iso to /var/TKLC/upgrade folder.

b) 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/repository directory. Store the ISO

file to /var/TKLC/upgrade directory. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure Adding ISO Images to the PM&C Image Repository

c) Download the following files from Oracle Download center and copy them to /var/TKLC/upgrade   folder:

- For WebLogic 10.3.5.0 product
  - o wls1035_generic.jar
  - o jrockit-jdk1.6.0_45-R28.2.7-4.1.0-linux-x64.bin.

6) **Mount ISO**

As root, run:

```
# mount -o loop iso_path /mnt/upgrade
```

where iso_path is the absolute path of the NSP ISO image, which includes the name of the image (starting with /var/TKLC/upgrade).

7) **Copy bulkconfig**

a) Login as root user on the Apache Box.
b) Copy the bulkconfig file from Apache box to /root directory.

8) **Upgrade Weblogic Product**

a) Login as root user , For an ISO file, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
# /mnt/upgrade/upgrade_weblogic.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted
```

b) Wait until the installation process is complete.

c) Analyze the installation log(/var/TKLC/log/upgrade/weblogic.log), the weblogic product is installed successfully message appears at the end of the log file.
If this message does not appear in the log file, contact Oracle Customer Care Center.

9) **Upgrade NSP**

a) Log in as root on the server to install the NSP application.

b) As `root`, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
# /mnt/upgrade/upgrade_nsp.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted
```

c) Wait for NSP installation to get complete. 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.

d) After the installation the server will restarts automatically. Log back in and review the NSP installation log (/var/log/nsp/install/nsp_install.log) and TPD upgrade log (/var/TKLC/log/upgrade/upgrade.log) for errors.
If NSP did not install successfully, contact the Oracle Customer Care Center.

Note: When user will login back to machine then a message will appear asking to accept or reject upgrade. Ignore this message for now. It will be automatically accepted when user will execute `post_upgrade_sanity_check.sh script during` *NSP Post-Upgrade Check (onebox and four box)*

5.1.4 Primary WebLogic Box

If not already done refer ***ReInstall Operating system*** **to reinstall the machine**

1) **Login as root user and run**:

```
# syscheck
```

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

Example ouput for a healthy system:

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

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

2) **Configure the server hostname**

a) As `root`, run:

```
# su - platcfg
```

b) Select **Server Configuration ➢ Hostname .**

c) Click **Edit.**

d) Type the NSP WebLogic Primary server hostname and click **OK**.
e) Return to the main **platcfg** menu.

3) Configure SNMP

a) From the main **platcfg** menu, select **Network Configuration➢SNMP Configuration➢NMS Configuration** and select **Edit > Add A New NMS Server**.
b) Type the IP address as **127.0.0.1** and **TEKELEC** as the community string and port number is not optional (port number 162) and then click **OK** and then **EXIT**
c) Click **YES** to restart alarm server and then press any Key to continue.
d) Exit the **platcfg** menu.

4) Temporary customer IP assignement

Refer section 4.1.5 Temporary customer IP assignment in E53508-01.docx

5) Copy NSP ISO

a) Copy NSP iso to /var/TKLC/upgrade folder.
b) 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/repository directory. Store the ISO
file to /var/TKLC/upgrade directory. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure How To Mount the ISO file from PM&C ISO Repository
c) Download the following files from Oracle Download center and copy them to /var/TKLC/upgrade folder:

- For WebLogic 10.3.5.0 product
    - wls1035_generic.jar
    - jrockit-jdk1.6.0_45-R28.2.7-4.1.0-linux-x64.bin.

6) Mount ISO

a) NSP ISO must be mounted on NSP server. *Refer How To Mount the ISO file from PM&C ISO Repository*. to mount the ISO on blade server.
b) To mount NSP ISO on RMS via ILO please refer How to mount the ISO file via iLO

7) Copy bulkconfig

a) Login as root user on the Apache Box.
b) Copy the bulkconfig file from Apache box to /root directory.

8) Upgrade Weblogic Product

a) Login as root user , For an ISO file, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
# /mnt/upgrade/upgrade_weblogic.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted
```

b) Wait until the installation process is complete.
c) Analyze the installation log(/var/TKLC/log/upgrade/weblogic.log), the weblogic product is installed successfully message appears at the end of the log file.
If this message does not appear in the log file, contact Oracle Customer Care Center.

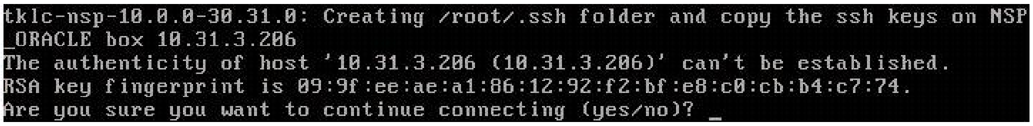
9) Upgrade NSP

a) Log in as root on the server to install the NSP application.
b) As `root`, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
# /mnt/upgrade/upgrade_nsp.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted
```

Note: During Primary box upgrade user will get a prompt asking for input as shown in below screen shot. User needs to enter yes in order to continue. After that a prompt will appear asking for password, user then needs to enter password for root user in order to continue.



```
tklc-nsp-10.0.0-30.31.0: Creating /root/.ssh folder and copy the ssh keys on NSP
_ORACLE box 10.31.3.206
The authenticity of host '10.31.3.206 (10.31.3.206)' can't be established.
RSA key fingerprint is 09:9f:ee:ae:a1:86:12:92:f2:bf:e8:c0:cb:b4:c7:74.
Are you sure you want to continue connecting (yes/no)? _
```

c) Wait for NSP installation to get complete. 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.

d) After the installation the server will restarts automatically. Log back in and review the NSP installation log (/var/log/nsp/install/nsp_install.log) and TPD upgrade log (/var/TKLC/log/upgrade/upgrade.log) for errors.

If NSP did not install successfully, contact the Oracle Customer Care Center.

Note: When user will login back to machine then a message will appear asking to accept or reject upgrade. Ignore this message for now. It will be automatically accepted when user will execute `post_upgrade_sanity_check.sh script during` *NSP Post-Upgrade Check (onebox and four box)*

5.2 Upgrade One-Box setup

If not already done refer *ReInstall Operating system* **to reinstall the machine and** *Remount NSP LUN(C-class blades only)* **for blade server only**.

1) Login as root user and run:

```
# syscheck
```

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

Example ouput for a healthy system:

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

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

2) **Configure the server hostname**

a) As `root`, run:

```
# su - platcfg
```

b) Select **Server Configuration ➢ Hostname** .

c) Click **Edit.**

d) Type the NSP server hostname and click **OK**.

e) Return to the main **platcfg** menu.

3) **Configure SNMP**

a) From the main **platcfg** menu, select **Network Configuration➢SNMP Configuration➢NMS Configuration** and select **Edit > Add A New NMS Server**.

b) Type the IP address as **127.0.0.1** and **TEKELEC** as the community string and port number is not optional (port number 162) and then click **OK** and than **EXIT**

c) Click **YES** to restart alarm server and then press any Key to continue.
d) Exit the **platcfg** menu.

4) Temporary customer IP assignement

Refer section 4.1.5 Temporary customer IP assignment in E53508-01.docx

5) Copy NSP ISO

a) Copy NSP iso to /var/TKLC/upgrade folder.

b) 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/repository directory. Store the ISO
file to /var/TKLC/upgrade directory. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure *8.5 Adding ISO Images to the PM&C Image Repository*.

c) Download the following files from Oracle Download center and copy them to /var/TKLC/upgrade folder:

- For Oracle Database 11.2.0.4 product
  - p13390677_112040_Linux-x86-64_1of7.zip
  - p13390677_112040_Linux-x86-64_2of7.zip
- For WebLogic 10.3.5.0 product
  - wls1035_generic.jar
  - jrockit-jdk1.6.0_45-R28.2.7-4.1.0-linux-x64.bin.

6) Mount NSP media

As root, run:

```
# mount -o loop iso_path /mnt/upgrade
```

where iso_path is the absolute path of the NSP ISO image, which includes the name of the image (starting with /var/TKLC/upgrade).

7) Copy bulkconfig

a) Login as root user on the NSP one Box.
b) Copy the bulkconfig file from backup directory(from the server on which you have copied during pre health check steps) to /root directory.

8) Upgrade Weblogic Product

a) Login as root user, For an ISO file, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
# /mnt/upgrade/upgrade_weblogic.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted
```

b) Wait until the installation process is complete.
c) Analyze the installation log(/var/TKLC/log/upgrade/weblogic.log), the weblogic product is installed successfully message appears at the end of the log file.
If this message does not appear in the log file, contact Oracle Customer Care Center.
d) Verify that /opt/oracle/backup directory and backup file in that directory exist.
Note: If backup folder or backup file is not available then do not proceed with upgrade and contact Oracle Customer Care Center.

9) Upgrade Oracle Product

a) As `root`, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
        # /mnt/upgrade/install_oracle.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted.
```

b) System will reboot after successful installation of oracle

c) Review the installation log (/var/TKLC/log/upgrade/oracle.log) for any errors. Oracle must be installed successfully.

If there are any errors, contact the Oracle PIC Design Support Team

10) **Verify NSP Backup**

a) Login as root user on the Oracle Box.

b) Verify the NSP backup on which the healthcheck was performed using "section 4.4 Check NSP Backup is valid " is present and is the latest backup. Execute the below command to find out the latest backup directory:

```
# ls -dtr /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 with upgrade and contact Oracle Customer Care Center.

11) **Upgrade NSP**

a) Log in as root on the server to install the NSP application.

b) For an NSP ISO file copied in /var/TKLC/upgrade run:

```
 # mount –o loop iso_path /mnt/upgrade
```

where iso_path is the absolute path of the NSP ISO image, which includes the name of the image (for example, /var/TKLC/upgrade/iso_file_name.iso).

- 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/repository directory. Store the ISO file to /var/TKLC/upgrade directory. If the ISO is not present in PM&C ISO repository.

b) As `root`, run:

Note: Run this procedure via iLO or through any non disconnectable console only.

```
# /mnt/upgrade/upgrade_nsp.sh
Note: /mnt/upgrade is the mount point where NSP ISO is mounted
```

d) Wait for NSP installation to get complete. 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.

e) After the installation the server will restarts automatically. Log back in and review the NSP installation log (/var/log/nsp/install/nsp_install.log) and TPD upgrade log (/var/TKLC/log/upgrade/upgrade.log) for errors.

If NSP did not install successfully, contact the Oracle Customer Care Center.

Note: When user will login back to machine then a message will appear asking to accept or reject upgrade. Ignore this message for now. It will be automatically accepted when user will execute post_upgrade_sanity_check.sh script during *5.5 NSP Post-Upgrade Check (onebox and four box)*

5.3 Upgrade A-Node (onebox and four box)

Warning: This step is applicable to one box and four box configurations.
Box: Onebox or Primary WebLogic boxes

1. **Upgrade Node A on One box or Four BoxCluster**

The following steps would install A-node on NSP OneBox or Weblogic Primary Box

a) Login as **root** user on the on NSP **One Box** server or **WebLogic Primary** server.

b) Insert the XMF DVD to the cdrom.

.

Note: However you are using the xMF iso for E5-AppB (TPD5.5) for the XMF upgrade you will need to use the xMF iso for HP (TPD6.5) server for this procedure

c) **If** ISO is available copy the ISO to NSPOne Box or Weblogic Primary server at some location.

d) Execute as root user the following command.

As root run:

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

e) When asked for ISO, provide the complete ISO path `/var/TKLC/upgrade/<isoname.iso>`

f) Type `yes` to confirm

g) No reboot needed

5.4 Post-Upgrade Settings (onebox and four box)

Warning: This step is applicable to onebox and four box configurations.
Box: Onebox or Primary WebLogic boxes

1. Configure Apache HTTPS Certificate (Optional)

a) Copy the files `server.crt` and `server.key` that are provided by the customer to `/root`

b) From platcfg root menu navigate to **NSPConfiguration ⊙ Configure Apache HTTPS Certificate**

This would install certificate provided by customer

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

<u>Disable access to HTTP</u>

a) Open a terminal console and Login as a root user on NSP One-Box server or NSP Primary WebLogic server server (Four-Box)

b) Enter the plactf menu

```
# su - platcfg
```

c) Navigate to **NSP Configuration ⊙ Enable HTTP Port ⊙ Edit**

d) Select **NO** and press **Ok** to enable access again to HTTP

e) Open a terminal console and Login as a root user on NSP One-Box server or NSP Primary WebLogic server server (Four-Box)

f) Enter the platcfg menu. As `root` run:

```
# su - platcfg
```

g) Navigate to **NSPConfiguration ⊙ Enable HTTP Port ⊙ Edit**

h) Select **YES**YES and press **Ok**

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 appliactions 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

NSP server (One-box) or NSP Primary & Secondary box in case of NSP 4 box.

a) Open a terminal window and log in as root

b) Enter the **platcfg** menu. As root, run: # su - platcfg

c) Select **NSP Configuration ► SMTP Configuration.**

d) Select **Edit.**

e) Type the IP address of the SMTP server and click **OK.**

f) The host file for the alias used in the WebLogic Mail service is updated.

g) Exit the platcfg menu

5. Transfer Ownership of TklcSrv 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 `TklcSrv` user.
b) Navigate to **security application ⊙ Transfer ownership value**
c) Transfer all the TklcSrv object to and other user (tekelec for example)

6. To enable or disable the legacy feeds refer the 909-2247-01 Maintenance guide when needed. (Optional)

Note: Refer also to the maintenance guide to convert the feeds in backaward compatible mode.

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

Note: By default NSP keep existing alarm classification .

a) Open a terminal window and log in as `root` user on NSP server (one box) or Oracle box (4box) .

b) Change user to Oracle and execute given command with NSP database sql user and password.

```
# su - oracle

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

5.5 NSP Post-Upgrade Check (onebox and four box)

Box: Onebox /Four Box

1. Open a terminal window and log in as root on the NSP One-box or the Primary server (Four-box).

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 NSP 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

- Oracle em console connectivity is OK

- The disk partition includes the following lines, depending on whether rackmount or blades setup:

• If rackmount, the output contains the following lines:

```
/dev/sdc1                        275G  4.2G  271G   2% /usr/TKLC/oracle/ctrl1

/dev/sdb1                        825G  8.6G  817G   2% /usr/TKLC/oracle/oradata

/dev/sdd1                        275G  192M  275G   1% /usr/TKLC/oracle/backup
```

Note: The lines must begin with the /dev/cciss/c1d*p1 designations; the remaining portion of the lines may differ.

• If blades, output contains following lines:

```
/dev/mapper/nsp_redo_vol 69G 4.2G 61G 7% /usr/TKLC/oracle/ctrl1
/dev/mapper/nsp_data_vol 413G 76G 316G 20% /usr/TKLC/oracle/oradata
/dev/mapper/nsp_backup_vol 138G 9.2G 121G 8% /usr/TKLC/oracle/backup
```

• If extended dictionaries exists, log shall include processing results to attach extended dictionary to a base protocol dictionary (for further protocol upgrade and ProTrace EPI) and calculation of a partial dictionary defining specific part. If extended dictionary is not used in any dataflow processing or does not contains all attributes of base dictionary, nothing is done.

5.6 NSP Backup (onebox and four box)

Warning: This step is applicable to onebox and four box configurations.
Box: Onebox or Primary WebLogic box

This procedure describes how to perform a backup from a NSP successfully upgraded in order to avoid restore the backup from previous release in case you would face in issue while the xMF and IXP 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 Weblogic Primary server or one BOX 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 4.4 Check NSP backup is Valid in order to make sure everything went fine.

Once the backup is complete, move this backup to some other server. In case of Four Box configuration, the user will be required to login to Oracle Box and 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

01 00 * * *  rm -rf /tekelec/backup`date
\+\%u`;/usr/TKLC/TKLCmf/bin/backup_config backup`date \+\%u` >
/tekelec/TKLCmf/runtime/run/log/backup`date \+\%u`.log
```

5.7 Upload xDR Builder ISO to NSP (onebox and four box)

Warning: This step is applicable to onebox and four box configurations.
Box: Onebox or Primary WebLogic box + workstation browser

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

Note 1: In case of failure in this step this is not blocking for the xMF upgrade but only for the IXP. This will give some time to Design Support to investigate the reason of this over the day.

Note 2: PIC supports IXP subsystems with 32 and 64 bit platform architecture. For an IXP subsystem of particular platform architecture, xDR builder ISO supporting corresponding platform architecture will be required.

1. **Install Builder ISO on NSP**

   a) Copy the xDR builder ISO to the NSP primary Weblogic server or insert xDR Builder CD-ROM.

   b) Login to the NSP primary Weblogic server or NSP One-box 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 NSP.**

   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 TklcSrv 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 7.3 Centralized xDR Builder upgrade 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 IXP 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.

6 xMF Major Upgrade

6.1 xMF Pre-Install Configuration

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

6.1.1 ReInstall Operating system on xMF server

a) **Refer** *ReInstall Operating system* **to reinstall the machine**

6.1.2 xMF Pre-Install Configuration

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

6.1.2.1 Temporary xMF customer IP assignment

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

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

Configure Vlan tagging and assign ip address in case of IMF

a) Login via ILO, MRV, OOBM or RMM to server as root

b) Execute following commands:

```
# modprobe 8021q

# vconfig add eth01 200

# ifconfig eth01.200 <CUST IP ADDRESS> netmask <MASK>

# route add default gw <DEFAULT ROUTE IP ADDRESS>
```

Configure Vlan tagging and assign ip address in case of PMF

a) Login via ILO, MRV, OOBM or RMM to server as root

b) Execute following commands:

```
# ifconfig eth01<CUST IP ADDRESS> netmask <MASK>

# route add default gw <DEFAULT ROUTE IP ADDRESS>
```

6.1.2.2 Copy ISO

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

6.1.3 Configure xMF

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

Note: This procedure must be executed on all of the IMF and PMF servers.

1. **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 IMF 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 PMF:

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

h) Select Exit.

6.2 xMF Pre-Install Healthcheck

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

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

```
# syscheck
```

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

```
Example ouput for a healthy system:
Running modules in class disk... OK
Running modules in class proc... OK
Running modules in class system... OK
Running modules in class hardware... OK

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

6.3 Install xMF

This procedure describes how to install the xMF 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 xMF application.

2. **Restore XMF configuration**

   a. Log in to the NSP 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 XMF on which the restore is to be done.

b. Once the script is executed successfully the archieve file will be restored at /var/TKLC/backup/ directory on xMF.

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

3**. 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.

Note: In case of TPD 5.5, the early checks may fail if the upgrade is not attempted from the non disconnectable media, so before attempting the next upgrade remove the “UNKNOWN” entry from “/usr/TKLC/plat/etc/platform_revision” file.

6.4 Sync NSP with xMF

1. **Set VIP**

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

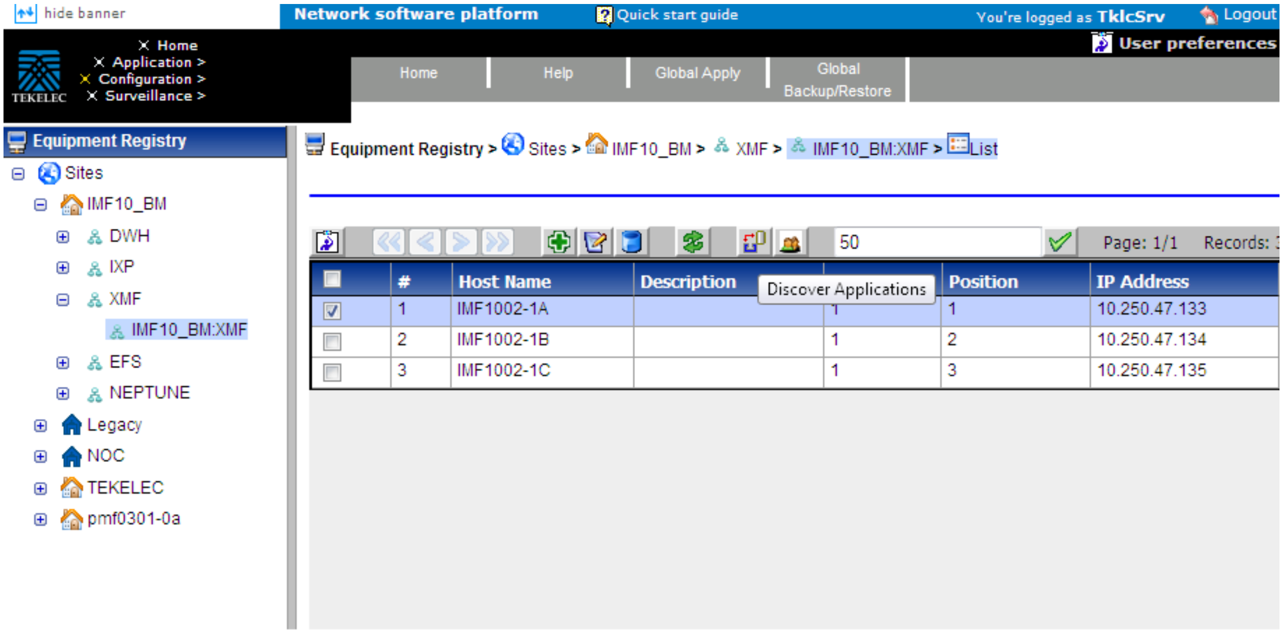
As cfguser run:

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

2. **Discover xMF Application on NSP**

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 XMF subsystem to synchronize by clicking on XMF under the correct Site name.
f) This will list the subsystem in the table
g) Select the xMF server and click on Discover Applications. The discover applications action should be done for each xMF server in the sub-system.



□	#	Host Name	Description	Discover Applications	Position	IP Address
☑	1	IMF1002-1A		1	1	10.250.47.133
□	2	IMF1002-1B		1	2	10.250.47.134
□	3	IMF1002-1C		1	3	10.250.47.135

3. **Apply Change**

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 NSP server. If VIP address is accessible from IMF servers but is not accessible from NSP, then it may be due to Cisco switch ARP table, refer to procedure **Flush ARP table** in Installation document.

6.5 xMF Post-Sync Healthcheck

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

The script gathers the healthcheck information from each server in the xMF subsystem or from standalone server. The script should be run from only on one server of the XMF 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. Open a terminal window and log in as cfguser on any server in the xMF subsystem or standalone server.
2. Run the automatic healthcheck script.

```
$ analyze_subsystem.sh
```

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, contact the Tekelec Customer Care Center.

   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 TPD VERSION: 3.3.8-
11:28:59:       63.25.0 XMF VERSION:    [  60.6.7-2.1.0 ]
11:28:59:       Checking disk free space
11:28:59:       No disk space issues found
11:28:59:       Checking whether ssh keys are exchanged among machines in frame this
11:28:59:       can take a while
11:29:08:
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!
```

7 IXP Major Upgrade

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

7.1 Install Operating system

Refer *ReInstall Operating system* to reinstall the machine

7.2 IXP Pre-Install Configuration

This procedure describes how to configure IXP 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:

```
# hpacucli ctrl all show
```

Example output:

```
# hpacucli 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:

```
# hpacucli 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:

```
# hpacucli 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 output:

```
0_oracle_data (3600c0ff000d825e6c7508d4f01000000) dm-8 HP,MSA2012fc
[size=1.4T][features=1 queue_if_no_path][hwhandler=0][rw]
\_ round-robin 0 [prio=2][active]
 \_ 0:0:0:1 sda        8:0   [active][ready]
 \_ 1:0:0:1 sdc        8:32  [active][ready]
0_oracle_index (3600c0ff000d82539cc6a8d4f01000000) dm-9 HP,MSA2012fc
[size=1.4T][features=1 queue_if_no_path][hwhandler=0][rw]
\_ round-robin 0 [prio=2][active]
 \_ 0:0:1:2 sdb        8:16  [active][ready]
 \_ 1:0:1:2 sdd        8:48  [active][ready]
```

Make sure the LUN number are the one expected per the engineering. The LUN is the number highlited in yellow in the example

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

Note: All the servers in an IXP 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) Enter the **platcfg menu**.
As root, run:

```
# su - platcfg
```

b) Select **Network Configuration -> Network Interfaces**.
c) Depending on the H/W, edit an existing interface or create a new one:

- On RackMount server, select **Edit an Interface**:
  (i) Select **eth01**
  (ii) Press **Edit**
  (iii) Don’t fill **MTU**; don’t change **GRO** option; select **none** for **BootProto** and press **OK**
  (iv) Press **Yes** to configure the IP address
  (v) Select **IPv4**
  (vi) Select **Add Address** and press **OK**

(vii) Continue with next step

- On C-Class Blade server, click **Add an Interface**:
  (i) Select **Vlan** and press **OK**
  (ii) Set **3** as **VLAN ID**; select interface **bond0**; press **OK**
  (iii) Don't fill **MTU**; select **none** for **BootProto** and press **OK**
  (iv) Press **Yes** to configure the IP address
  (v) Continue with next step

b) Enter the host's IP address:

- Fill in **IP Address**
- Fill in **Netmask**
- Select **yes** for **Start on Boot**
- Press **OK**

c) **Exit** the platcfg menu.

7.3 Install IXP

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

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

Note: Run this procedure via iLO.

1) **Restoring IXP**

a) Log in to the NSP 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 IXP on which the restore is to be done.

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.

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 IXP 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.

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

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.

Information note: At this step, for BL460 G6 servers, the default gateway is not set, thus, remote access is only possible though the iLO (the gateway will be set during Customer integration).

5) **Analyze the installation log**
Review the installation log (/var/TKLC/log/upgrade/upgrade.log) for any errors.
If there are any errors, contact the Oracle PIC Design Support Team

6) **Set VIP**
As cfguser, run on 1A server only:

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

7.4 IXP 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, then contact Oracle Customer Care Center.

7.5 Integrate Customer Network

This procedure describes how to integrate the IXP subsystem post-manufacturing customer network. This procedure uses the /root/bulkconfig file as an input for the customer network integration. Before you perform this procedure, make sure you have read and are familiar with the IXP Bulkconfig File Description.
This procedure is run from the iLO.

1) **Update the bulkconfig file (if IP addresses need to changed)**
   a) Log in on the iLO of any IXP server in the IXP 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 IXP 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 IXP 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, contact the Tekelec Customer Care Center.

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 DataBroker and CSV streaming feeds).

4) Discover the IXP 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.

7.6 Install xDR Builders

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

1) Associate the xDR Builders RPM with the IXP subsystem

m) Open a web browser and log in as TklcSrv on the NSP application interface.
n) Open the Upgrade Utility.
o) Click View Builder RPM Status in the left tree. A list of the IXP subsystems appears.
p) Select one or more IXP subsystems and click Associate RPM Package. A list of Builder RPMs that are uploaded in NSP appears.
q) 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 contact the Tekelec Customer Care Center.

2) Apply the configuration to the IXP 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 IXP

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 IXP 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 IXP subsystem is associated with the IXP 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 IXP subsystems and click Install RPM Package. If the installation is successful, the Install status changes to OK. If the installation fails contact the Oracle Customer Care Center.

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.

7.7 IXP Subsystem Healthcheck

This procedure describes how to run the automatic healthcheck of the IXP subsystem.

1) Open a terminal window and log in on any IXP server in the IXP 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 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
```

7.8 Upgrade DTO Package

Whenever you will install or upgrade IXP 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 NSP 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 IXP subsystem from which this DataWarehouse server is reachable.
As **cfguser** run:

```
$ iqt -L DatawareHouse
```

Note down Login, Password, Host IP address and Instance name of the DataWarehouse.

b) Connect to the DataWarehouse.
As **cfguser** run:

```
$ sqlplus user/password@ip_address/instance
```

Where *user*, *password*, *ip_address* and *instance* are the values received in previous step.

c) Check the DTO package version:

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

If the DTO package upgrade is needed continue with the next step. Quit the SQL console.

```
SQL> quit
```

2) **Upgrade DTO package**

a) As **cfguser** from any server of the IXP subsystem run:

```
$ cd_oracle_utils
$ UpgradeDTOPkg.sh DWH_connection SYS_connection DWH_user
```

where:

- *DWH_connection* is the Oracle DWH connection string (*user/password@ip_address/instance*)
- *SYS_connection* is the Oracle SYS connection string (SYS/*SYS_password@ip_address/instance*)
Note: refer to TR006061 for the default value for the SYS password.
- *DWH_user* is the DWH user name (optional, default value: 'IXP')

WARNING

Take care the user and password are case sensitive

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 user/password@ip_address/instance
```

      Where *user*, *password*, *ip_address* and *instance* are the values 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
```

7.9 Capacity Management KPIs installation

Capacity Management is a statistical session is generated with a dedicated xDR builder.
It provides very detailed self-surveillance data which can be better analyzed after selection and aggregation.
Derived statistical data are produced in real time (periodicity at the minute, quarter of hour and hour).
These statistical results are stored as regular xDR, which allows to manage this with standard PIC tools (such as ProTrace or ProPerf).
They globally provide system activity information in real time and an historical, traffic volume and verify the accuracy according to licenses.

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

7.9.1 Installation Procedures for Capacity Management standard KPIs

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

1) CapacityManagement statistical session deployment
   a) All elements such as dedicated streams and DataFlows for this statistical session are automatically created as part of system deployment.
      Naming convention makes that needed elements will contain *FlowMonitor* in the name (generally as suffix).
   b) Each time a new equipment such as IXP or xMF will be added to the system, it will be taken into account by CCM to create all new needed *FlowMonitor* elements. This mechanism will be done by a check at each configuration changes.
   c) You must check whether these elements have been correctly deployed or not (by using CCM and verifying presence or not of dedicated streams and DFP).
      If not, please contact Support team in order to have the needed elements deployed for further usage of *Capacity Management*.
2) ProTraq templates deployment
   a) A set of ProTraq templates is provided.
      3 configurations must be deployed (no automatic feature for this operation):
      - **PIC_UsageStat_Mn**: applied on *CapacityManagement*; provides consolidation / conversion of input Mbps for probed acquisition (PMF), integrated acquisition (IMF) and mediation (IXP) over 1 mn.

        Refer to PIC 10 installation guide E53508 Section 16 APPENDIX: Capacity Management ProTraq configurations

- **PIC_UsageStat**: applied on *PIC_UsageStat_Mn* result stat session; Agregation of PIC_UsageStat_Mn results over 1 hour. Provides average, minimum, maximum throughput.

  Refer to PIC 10 installation guide E53508 Section 16 APPENDIX: Capacity Management ProTraq configurations
- **PIC_ActivityStat**: applied on *CapacityManagement*; Aggregation of key output data flows over 1 hour, per destination for xMF and per final XB for IXP in Kbps and efficiency

  Refer to Capacity management good practices(Doc ID 1683859.2) on My Oracle Support

b) These ProTraq templates configurations must be applied on the basic statistical session *CapacityManagement* which is part of the standard deployment.

c) Activate the configurations

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

For deeper usages of *Capacity Management* please refer to the dedicated document (e.g. IXP and xMF troubleshooting guides).

7.10 IXP Post-Integration Configuration (Optional)

This section contains various optional post-integration configuration procedures.

7.10.1 DataBroker and CSV streaming feeds

This procedure describes how to integrate a DataBroker server into an IXP subsystem. Data Broker streaming feeds write files on customer servers providing NFS shared directories.
That same procedure is to be followed to integrate a CSV server into an IXP 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 IXP 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 IXP subsystem or which is part of another IXP 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 IXP's `cfguser` user. If the user `cfguser` also exists on the sharing server, with the same UID as on the IXP 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 IXP server); add as many lines as IXP 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 IXP side
Note: These steps are to be executed on each IXP 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.

7.10.2 Delivery Network Failure and Recovery (DataBroker)

This application shall be available 24 hours a day, seven days per week, except for minimal downtime due to planned production maintenance.
Note: Even if this procedure is applicable to all the IXP servers, it is not recommended to apply it for other purposes than DataBroker streaming feed, for which only it has been tested.
Configure IDB to extend 24 hours of xDRs can be kept in the DTS buffers. As cfguser on IXP primary , run:

```
# IxpExtendDataBroker24hrs.sh
```

Result with 3 IXP servers:

```
Testing host is primary ................
Host is primary
Testing user is cfguser ................
User is cfguser
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1b    === changed 1 records ===
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1c    === changed 1 records ===
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1a    === changed 1 records ===
```

7.11 NSP Backup (onebox and four box)

Warning: This step is applicable to onebox and four box configurations.
Box: Onebox or Primary WebLogic box

This procedure describes how to perform a backup from a NSP successfully upgraded in order to avoid restore the backup from previous release in case you would face in issue while the xMF and IXP 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 NSP backup, move back the backup which was copied to some other server as per steps mentioned in section 5.6. In case of Four box configuration, move this backup to Oracle box. Below is the location where backup is to be moved in case of One Box or Four Box (Oracle Box)

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

As `root` run on Weblogic Primary server or one BOX 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 4.4 Check NSP backup is Valid 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

01 00 * * *  rm -rf /tekelec/backup`date
\+\%u`;/usr/TKLC/TKLCmf/bin/backup_config backup`date \+\%u` >
/tekelec/TKLCmf/runtime/run/log/backup`date \+\%u`.log
```

7.12 Unset Configuration on NSP (onebox and four box)

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

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

a) Open a web browser and log in to the NSP application interface as TklcSrv user.

b) Navigate to security application ⦿ Filter access

c) Select None for Restricted configuration setting.

d) Apply modification.

8 Appendix : Knowledge Base Procedures

8.1 ReInstall Operating system

Estimation: 30 mins (In case of blade server)
50 mins (in case of rackmount server)

a) Install the operating system.

- For RMs HP G6 server follow steps from PIC 10 Maintenance guide, E53511 section 8.2 Install Operating System on G6 Rackmount Servers

- For RMs HP Gen8 server follow steps from PIC 10 installation guide, E53508 section 9 APPENDIX: Rackmount BIOS Settings and Server IPM

- For C-class blade steps from PIC 10 installation guide, E53508 section 11.5 IPM Servers Using PM&C Application and than section 11.6 Additional configuration step after IPM

b) for NSP Oracle server resize /var/TKLC partition by following the steps from PIC 10 installation guide, E53508 section 3.4

8.2 Remount NSP LUN(C-class blades only)

This procedure describes different steps to follow to remount the logical volumes from MSA2012fc to NSP server of one box server or Oracle server

Prerequisite:

The NSP one box server/ Oracle server configuration must be IPM, with network and other system parameters set, the same way as for a fresh install.

Password of platcfg user must be already known.

1. **Login**

a) Login as **root** user on the NSP server for onebox/ Oracle server.

2. **Retrieve LUN numbers of logical volumes**

a) As root run:

```
# multipath -ll
```

The result will display 2 blocks of lines starting with “mapth0” and “mapth1”

Example:

```
mpath0  (3600c0ff000d5809fb180cc4901000000) dm-6 HP,MSA2012fc

[size=70G][features=0][hwhandler=0]

\_ round-robin 0 [prio=1][active]

\_ 0:0:0:37 sdc 8:32  [active][ready]

\_ round-robin 0 [prio=1][enabled]

\_ 1:0:0:37 sdd 8:48  [active][ready]

mpath1  (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc

[size=419G][features=0][hwhandler=0]

\_ round-robin 0 [prio=1][active]

\_ 0:0:1:36 sda 8:0   [active][ready]

\_ round-robin 0 [prio=1][enabled]

\_ 1:0:1:36 sdb 8:16  [active][ready]

mpath2  (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc

[size=139G][features=0][hwhandler=0]

\_ round-robin 0 [prio=1][active]

\_ 0:0:1:35 sde 8:64   [active][ready]

\_ round-robin 0 [prio=1][enabled]

\_ 1:0:1:35 sdf 8:80  [active][ready]
```

b) The lun# is the 4th number in the 4th and 6th line of each block, here in the example **37** for mpath0, **36** for mpath1 and **35** for mpath2

Lun# for REDO is the one in the block containing **[size=70G]** (37 in example)

Lun# for DATA is the one in the block containing **[size=419G]**(36 in example)

Lun# for BACKUP is the one in the block containing **[size=139G]**(35 in example)

3. Recreate mapping to SAN REDO volume

a) Execute the following command, replacing lun# (37 in example), by the one retrieved for REDO. As root run:

```
root# tpdProvd --client --subsystem=TPD::SOAP::Storage
addVolumeInfo lun 37 name nsp_redo_vol mount
/opt/oracle/ctrl1
```

b) When prompted for Login on Remote with the user platcfg, enter password for platcfg user . Refer to Teklec Default Passwords ,TR006061 to get the default value.

c) After completion, the output must show:

```
<result>

1
```

```
</result>
```

4. Recreate mapping to SAN DATA volume

a) Execute the following command, replacing lun# (36 in example), by the one retrieved for DATA. As root run:

```
# tpdProvd --client --subsystem=TPD::SOAP::Storage
addVolumeInfo lun

36 name nsp_data_vol mount /opt/oracle/oradata
```

b) When prompted for **Login on Remote** with the user `platcfg,` enter password for platcfg user from the Teklec Default Passwords ,TR006061.

c) After completion, the output must show:

```
<result>

1

</result>
```

5 Recreate mapping to SAN BACKUP volume

a) Execute the following command, replacing lun# (35 in example), by the one retrieved for DATA. As root run:

```
# tpdProvd --client --subsystem=TPD::SOAP::Storage
addVolumeInfo lun

35 name nsp_backup_vol mount /opt/oracle/backup
```

b) when prompted for **Login on Remote** with the user `platcfg,` enter password for platcfg user from the Teklec Default Passwords ,TR006061

c) After completion, the output must show:

```
<result>

1

</result>
```

6. Check the volume names

a) As root run:

```
root# multipath -ll
```

b) It will display 3 blocks of lines starting with **mapth0**, **mapth1** and **mpath2**
Example:

```
nsp_redo_vol (3600c0ff000d5809fb180cc4901000000) dm-6 HP,MSA2012fc

[size=70G][features=0][hwhandler=0]

\_ round-robin 0 [prio=1][active]

\_ 0:0:0:37 sdc 8:32  [active][ready]

\_ round-robin 0 [prio=1][enabled]

\_ 1:0:0:37 sdd 8:48  [active][ready]
```

```
nsp_data_vol (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc

[size=419G][features=0][hwhandler=0]

\_ round-robin 0 [prio=1][active]

\_ 0:0:1:36 sda 8:0   [active][ready]

\_ round-robin 0 [prio=1][enabled]

\_ 1:0:1:36 sdb 8:16  [active][ready]

nsp_backup_vol (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc

[size=139G][features=0][hwhandler=0]

\_ round-robin 0 [prio=1][active]

\_ 0:0:1:35 sde 8:64   [active][ready]

\_ round-robin 0 [prio=1][enabled]

\_ 1:0:1:35 sdf 8:80  [active][ready]
```

c) It should no longer show **mapth0**, **mpath1** and **mpath2**

7. Check the file system

a) As root run:

```
# fsck /dev/mapper/nsp_redo_vol
# fsck /dev/mapper/nsp_data_vol
# fsck /dev/mapper/nsp_backup_vol
```

8. Mount the volumes

a) As root run:

```
# mount -a
```

9. Verify the volumes

a) Actual values may change from example below:

```
# df –h

Filesystem           Size  Used Avail Use% Mounted on

/dev/mapper/vgroot-plat_root

                     496M  123M  349M  26% /

/dev/cciss/c0d0p1    122M  9.9M  106M   9% /boot


none                 4.0G     0  4.0G   0% /dev/shm

/dev/mapper/vgroot-plat_tmp

                    1008M   47M  910M   5% /tmp

/dev/mapper/vgroot-plat_usr

                     4.0G  1.1G  2.7G  30% /usr

/dev/mapper/vgroot-plat_var

                     496M   40M  431M   9% /var

/dev/mapper/vgroot-plat_var_tklc
```

```
                      4.0G   68M  3.7G   2% /var/TKLC
/dev/mapper/nsp_redo_vol
                     69G  4.2G   61G   7% /usr/TKLC/oracle/ctrl1
/dev/mapper/nsp_data_vol
                    413G  3.2G  389G   1% /usr/TKLC/oracle/oradata
/dev/mapper/nsp_backup_vol
                    138G  207M  130G   1% /usr/TKLC/oracle/backup
```

8.3 How to mount the ISO file via iLO

Refer to Platform 6.5 Configuration Procedure Reference 909-2249-001 Appendix H How to Attach an ISO Image to a Server Using the iLO

Now the ISO file is mounted on a target server as a virtual CD-ROM. Such new device will appear under `/dev/` directory.

To find the new virtual CD-ROM media run on a target server as `root`:

```
# getCDROMmedia
```

This will list a virtual CD-ROM media devices with the exact device name. Example output:

```
[root@ixp1977-1a ~]# getCDROMmedia
HP Virtual DVD-ROM:scd0
```

this record denotes virtual CD-ROM device `/dev/scd0` ready for any other operation.

8.4 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**

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

5. **Start portmap service**

   a) As `root` run:

```
# service portmap start
```

6. **Start nfslock service**

   a) As `root` run:

```
# service nfslock start
```

7. **Create ISO mount point**

   a) 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**

   a) 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
```

8.5 Adding ISO Images to the PM&C Image Repository

Refer to Platform 6.5 Configuration Procedure Reference 909-2249-001 Appendix 3.7.9

8.6 How to connect a server console using iL0 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->
```

Than 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.el6prerel6.0.1_80.32.0.x86_64 on an x86_64

hostname1368545964 login:
CentOS release 6.3 (Final)
Kernel 2.6.32-279.5.2.el6prerel6.0.1_80.32.0.x86_64 on an x86_64

hostname1368545964 login:
CentOS release 6.3 (Final)
Kernel 2.6.32-279.5.2.el6prerel6.0.1 80.32.0.x86 64 on an x86 64

hostname1368545964 login: root
Password:
```

8.7 PM&C 5.0 to 5.5 upgrade

Follow document 909-2281-001 PM&C 5.5 Incremental Upgrade for PM&C upgrade procedure.

8.8 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 E5308-01 Appendix G.1.7

For **each CISCO 3020** switch.

A. 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
```

9 Appendix: My Oracle Support (MOS)

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, 365 days a year.

10 Appendix: Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the Oracle Technology Network site at http://docs.oracle.com.

2. Under Applications, click the link for Communications.

   The Oracle Communications Documentation window opens with Tekelec shown near the top.

3. Click Oracle Communications Documentation for Tekelec Products.

4. Navigate to your Product and then the Release Number, and click the View link (the Download link will retrieve the entire documentation set).

5. To download a file to your location, right-click the PDF link and select Save Target As.