Oracle® Communications

Performance Intelligence Center

Incremental Upgrade Guide

Release 10.1.5

E56063 Revision 1

August 2015

Oracle Communications Performance Intelligence Center Incremental Upgrade, Release 10.1.5

CAUTION: Use only the guide downloaded from the Oracle Technology Network (OTN) (http://www.oracle.com/technetwork/indexes/documentation/oracle-comms-tekelec-2136003.html).
Before upgrading your system, access the My Oracle Support web portal (https://support.oracle.com) and review any Knowledge Alerts that may be related to the System Health Check or the Upgrade.

Before beginning this procedure, contact My Oracle Support and inform them of your upgrade plans.

Refer to Appendix B for instructions on accessing My Oracle Support.

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

[1] Platform 7.0 Configuration Procedures References, E53486, December 2014
[2] PM&C Incremental Upgrade Procedures, E45387, November 2014
[3] TVOE 3.0.0.0.0 Software Upgrade Procedure , E53018, June 2015
[4] PIC 10.1.5 Maintenance Guide, E56062, February 2015
[5] HP Solutions Firmware Upgrade Pack 2.2.8, E59723, March 2015
[6] Oracle Firmware Upgrade Pack, E54963, June 2014
[7] PIC 10.1.5 Installation Document, E56065, February 2015
[8] Tekelec Default Passwords ,TR006061
[9] Oracle Support Document 1984685.2 (Information Center: Upgrade Oracle Communications Performance Intelligence Center)
[10] PIC Hardware Guidelines

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 incremental upgrade procedures for the PIC system at Release 10.
This document is intended for use by internal Oracle manufacturing, PSE, SWOPS, and many times partners trained in software upgrade on both rack mount 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 rack mount 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

Refer PIC Hardware Guidelines

1.5.2 Software Requirements

The following software is required for the PIC 10.1.5 incremental 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 10.1.5 Maintenance Guide for detailed instruction.

Note: For specific versions and part numbers, see the PIC 10.1.5 Release Notice.

The following software is required for the PIC 10.1.5 incremental upgrade.

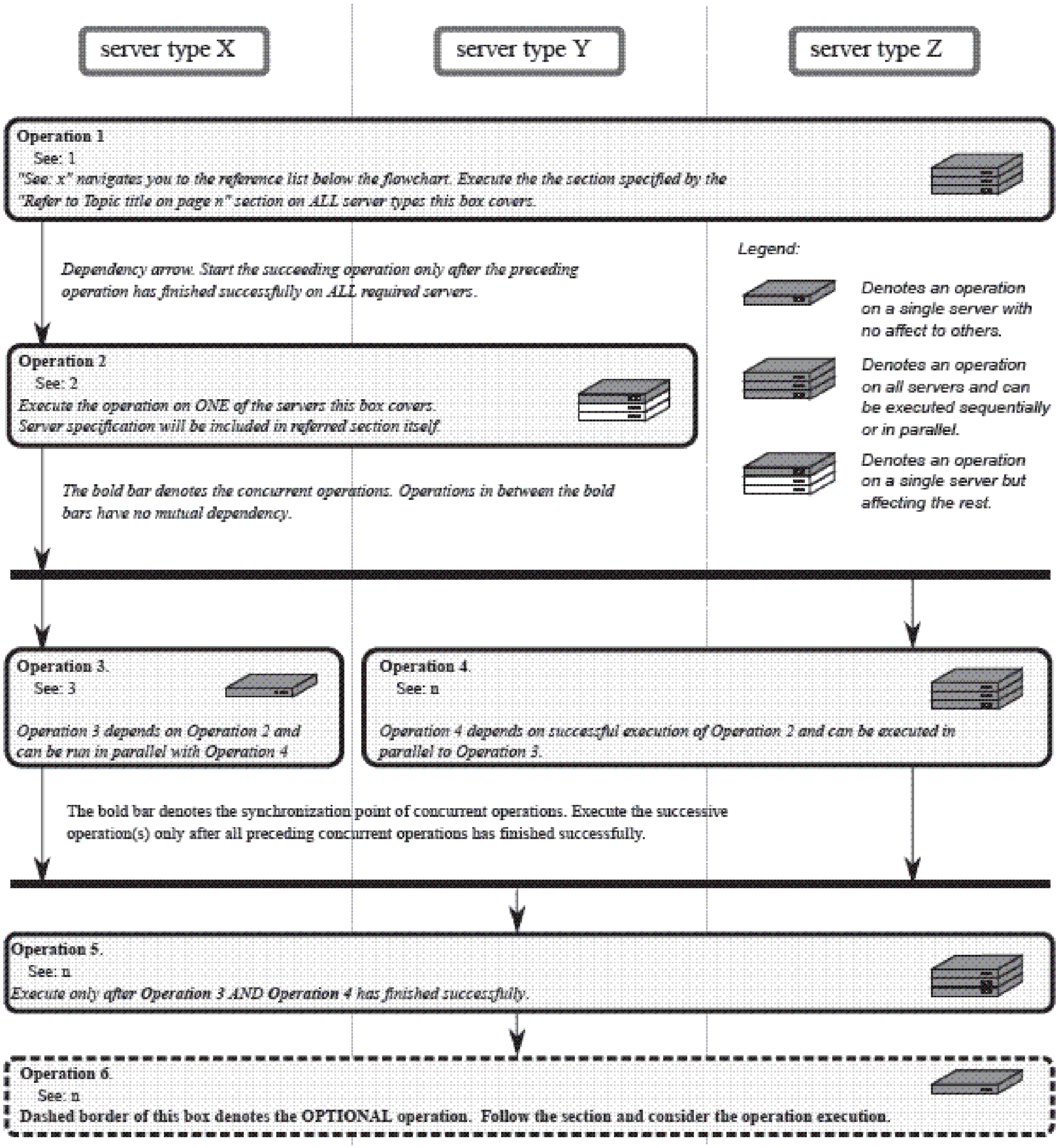
Oracle Communication GBU deliverables:

- Management Server
- Mediation Server
- Mediation Protocol
- Acquisition Server
- TADAPT
- Set of script to enable optional feature
- TPD
- TVOE (for blade only)
- PM&C (for blade only)

2 Incremental 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.

1. Refer to *Topic title* on page *n*.
2. Refer to *Topic title* on page *n*.
3. Refer to *Topic title* on page *n*.

2.2 PIC High-level Incremental Upgrade

This flowchart describes the PIC high-level incremental 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 incremental upgrade procedures are applicable to PIC systems installed in 10.1.5 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 incremental upgrade. The latest patch are listed on Oracle Support Document 1989320.2 (Information Center: Patches for Oracle Communications Performance Intelligence Center) and are available at Appendix B My Oracle Support

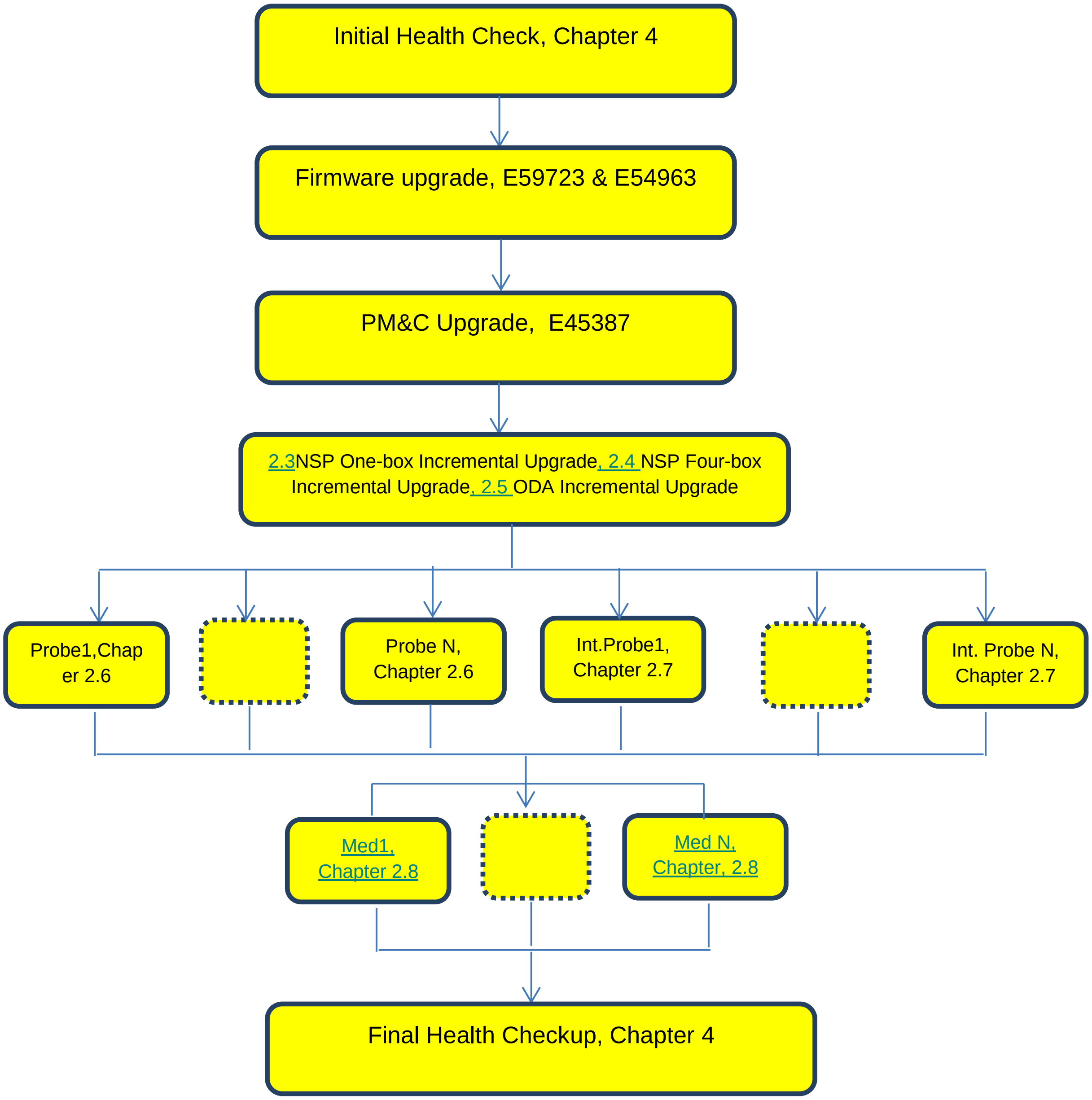
It is advised to have a look on the latest upgrade issue discovered after this manual was published on Oracle Support Document 1984685.2 (Information Center: Upgrade Oracle Communications Performance Intelligence Center)

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 incremental upgrade.
If running the PIC Incremental Upgrade on HP C-Class Blade platform the PM&C application must be upgraded first prior to PIC applications upgrade. Follow document **PM&C 6.5 Incremental Upgrade Procedure [2]**

The general upgrade strategy is as follows:

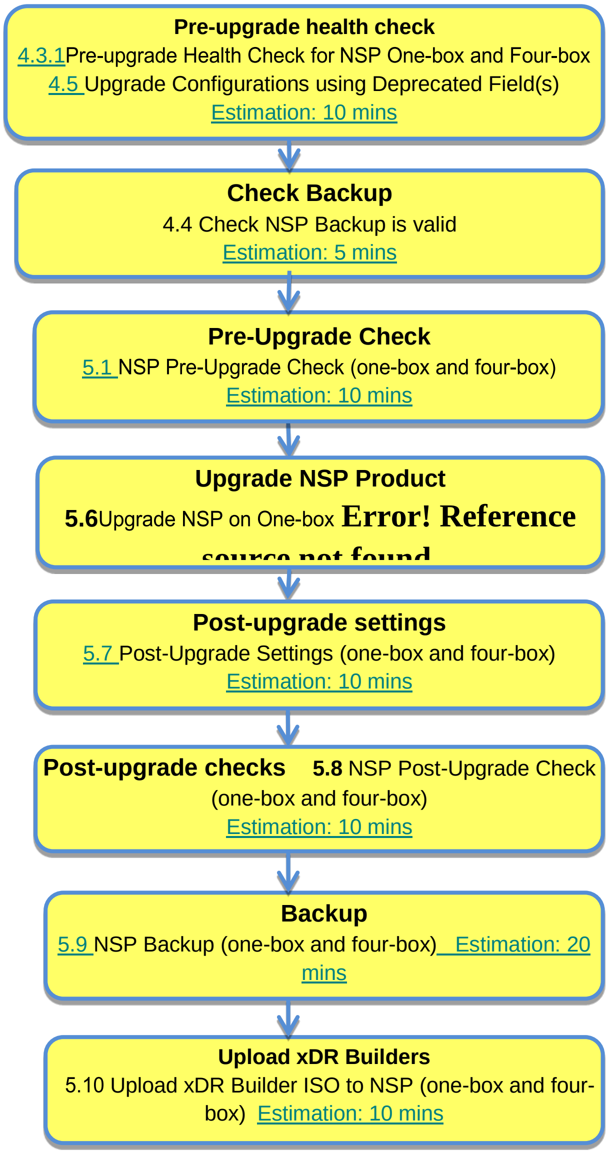
1. Initial health check at least 2 weeks before the planned operation in order to have time to replace defective hardware
2. Optional Firmware upgrade to the latest release available on the OSDC
3. PM&C Incremental upgrade and update the enclosure switches configuration
4. NSP upgrade (four-box or one-box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

Note: Firmware upgrade should be skipped for DWS and Management server deployed on ODA.


Initial Health Check, Chapter 4
Firmware upgrade, E59723 & E54963
PM&C Upgrade, E45387
2.3NSP One-box Incremental Upgrade, 2.4 NSP Four-box Incremental Upgrade, 2.5 ODA Incremental Upgrade
Probe1,Chapter 2.6
Probe N, Chapter 2.6
Int.Probe1, Chapter 2.7
Int. Probe N, Chapter 2.7
Med1, Chapter 2.8
Med N, Chapter, 2.8
Final Health Checkup, Chapter 4

2.3 NSP One-box Incremental Upgrade

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



Pre-upgrade health check
4.3.1Pre-upgrade Health Check for NSP One-box and Four-box
4.5 Upgrade Configurations using Deprecated Field(s)
Estimation: 10 mins

Check Backup
4.4 Check NSP Backup is valid
Estimation: 5 mins

Pre-Upgrade Check
5.1 NSP Pre-Upgrade Check (one-box and four-box)
Estimation: 10 mins

Upgrade NSP Product
5.6 Upgrade NSP on One-box **Error! Reference source not found**

Post-upgrade settings
5.7 Post-Upgrade Settings (one-box and four-box)
Estimation: 10 mins

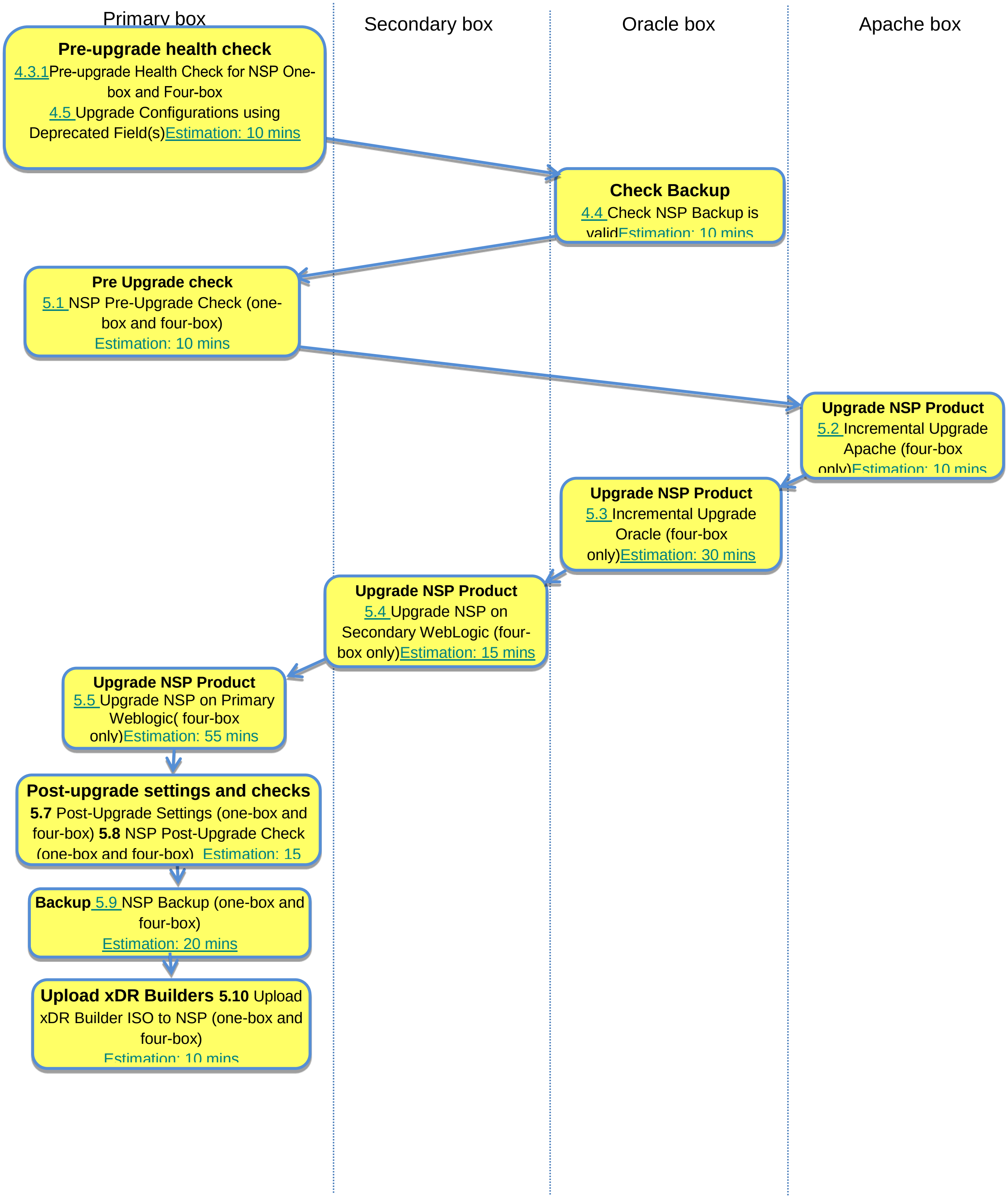
Post-upgrade checks **5.8** NSP Post-Upgrade Check (one-box and four-box)
Estimation: 10 mins

Backup
5.9 NSP Backup (one-box and four-box) Estimation: 20 mins

Upload xDR Builders
5.10 Upload xDR Builder ISO to NSP (one-box and four-box) Estimation: 10 mins

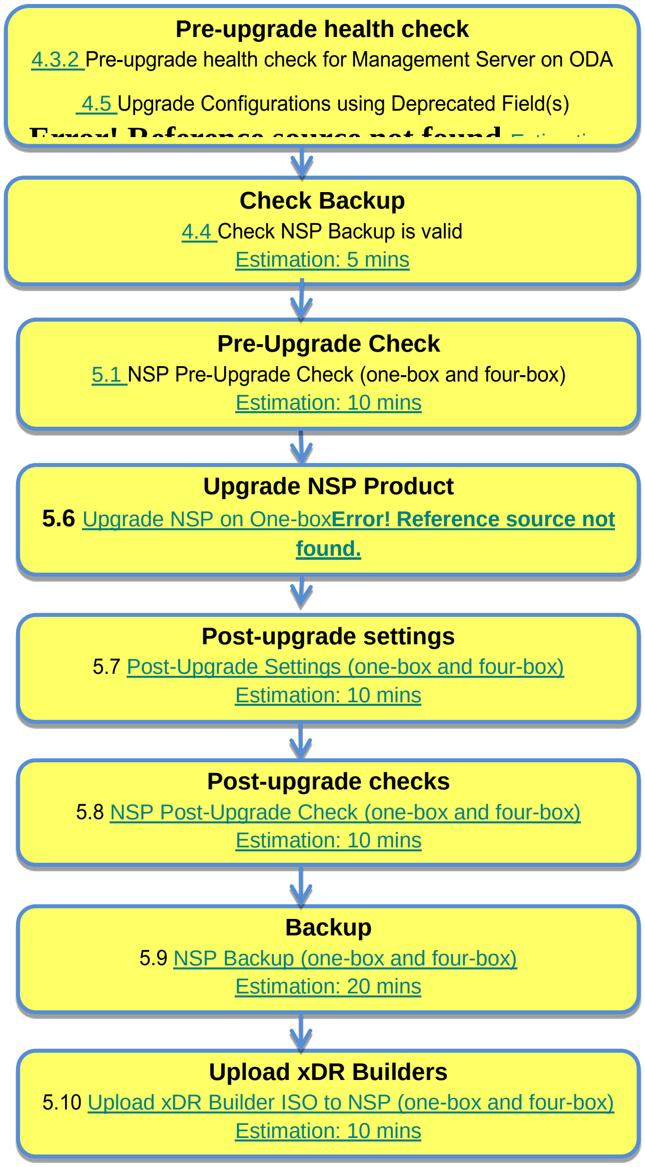
2.4 NSP Four-box Incremental Upgrade

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


Primary box
Secondary box
Oracle box
Apache box
Pre-upgrade health check
4.3.1Pre-upgrade Health Check for NSP One-box and Four-box
4.5 Upgrade Configurations using Deprecated Field(s)Estimation: 10 mins
Check Backup
4.4 Check NSP Backup is validEstimation: 10 mins
Pre Upgrade check
5.1 NSP Pre-Upgrade Check (one-box and four-box)
Estimation: 10 mins
Upgrade NSP Product
5.2 Incremental Upgrade Apache (four-box only)Estimation: 10 mins
Upgrade NSP Product
5.3 Incremental Upgrade Oracle (four-box only)Estimation: 30 mins
Upgrade NSP Product
5.4 Upgrade NSP on Secondary WebLogic (four-box only)Estimation: 15 mins
Upgrade NSP Product
5.5 Upgrade NSP on Primary Weblogic(four-box only)Estimation: 55 mins
Post-upgrade settings and checks
5.7 Post-Upgrade Settings (one-box and four-box) 5.8 NSP Post-Upgrade Check (one-box and four-box) Estimation: 15
Backup 5.9 NSP Backup (one-box and four-box)
Estimation: 20 mins
Upload xDR Builders 5.10 Upload xDR Builder ISO to NSP (one-box and four-box)
Estimation: 10 mins

2.5 ODA Incremental Upgrade

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



Pre-upgrade health check
4.3.2 Pre-upgrade health check for Management Server on ODA
4.5 Upgrade Configurations using Deprecated Field(s)
Error! Reference source not found. Estimati

Check Backup
4.4 Check NSP Backup is valid
Estimation: 5 mins

Pre-Upgrade Check
5.1 NSP Pre-Upgrade Check (one-box and four-box)
Estimation: 10 mins

Upgrade NSP Product
5.6 Upgrade NSP on One-box**Error! Reference source not found.**

Post-upgrade settings
5.7 Post-Upgrade Settings (one-box and four-box)
Estimation: 10 mins

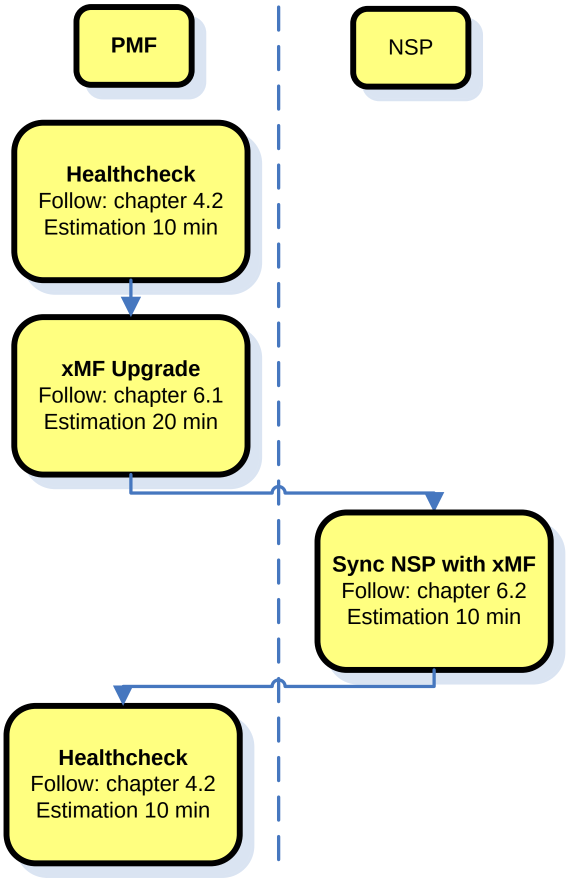
Post-upgrade checks
5.8 NSP Post-Upgrade Check (one-box and four-box)
Estimation: 10 mins

Backup
5.9 NSP Backup (one-box and four-box)
Estimation: 20 mins

Upload xDR Builders
5.10 Upload xDR Builder ISO to NSP (one-box and four-box)
Estimation: 10 mins

2.6 Probed Acquisition Incremental Upgrade

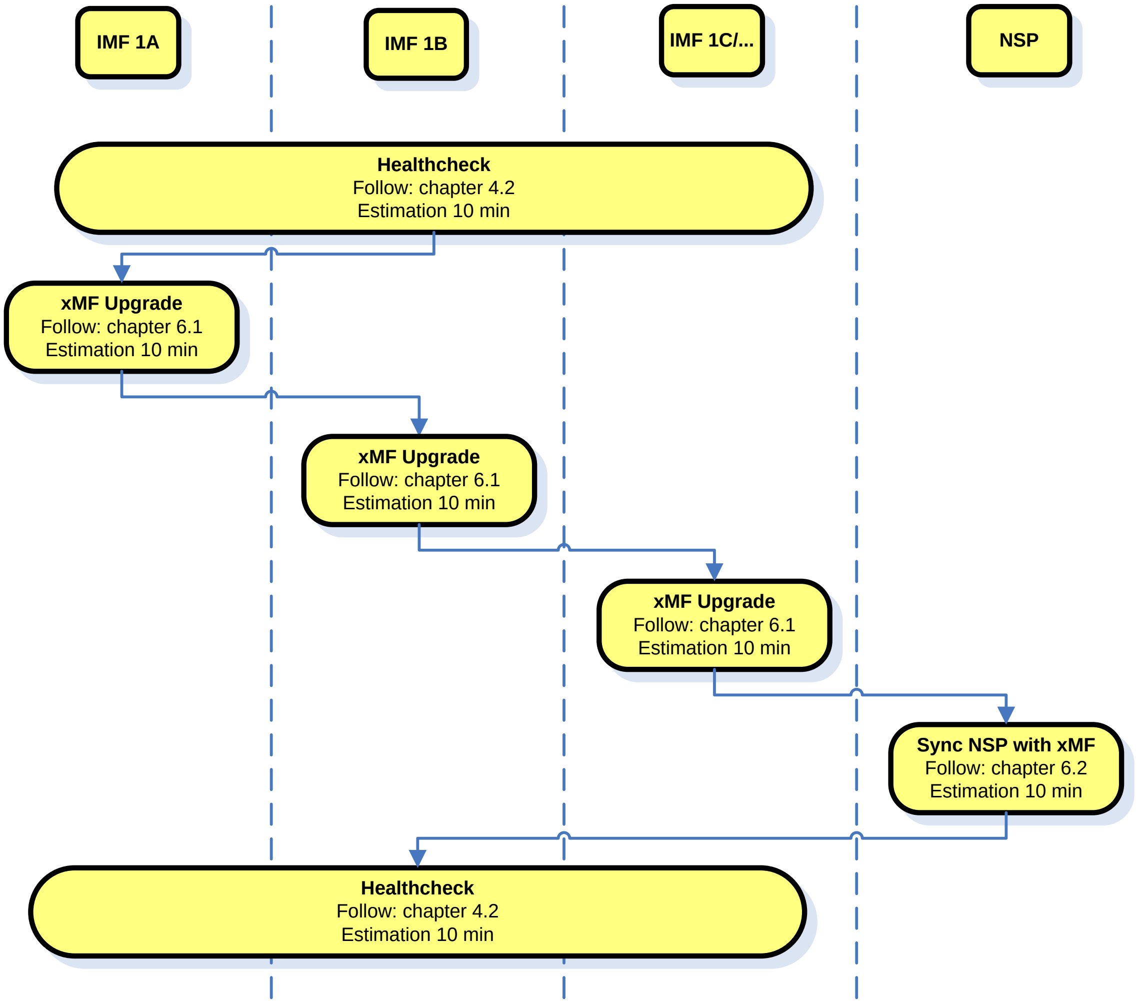
This flowchart depicts the sequence of procedures that must be executed to upgrade standalone Probed Acquisition Server.
The procedures depicted in the flowchart pertain to standalone Probed Acquisition server type.
Depending on the number of servers for a particular function, the required procedures depicted in the flowchart will need to be repeated.



2.7 Integrated Acquisition Serial Incremental Upgrade

This flowchart depicts the sequence of procedures that must be executed to upgrade the Integrated Acquisition Sub-system with minimum data lost.

Note: the HA won't be stopped during the incremental upgrade. However, in case of major upgrade of COMCOL or major changes in IDB schema that would require HA to be stopped, it is necessary to proceed with a major upgrade.



2.8 Mediation Incremental Upgrade

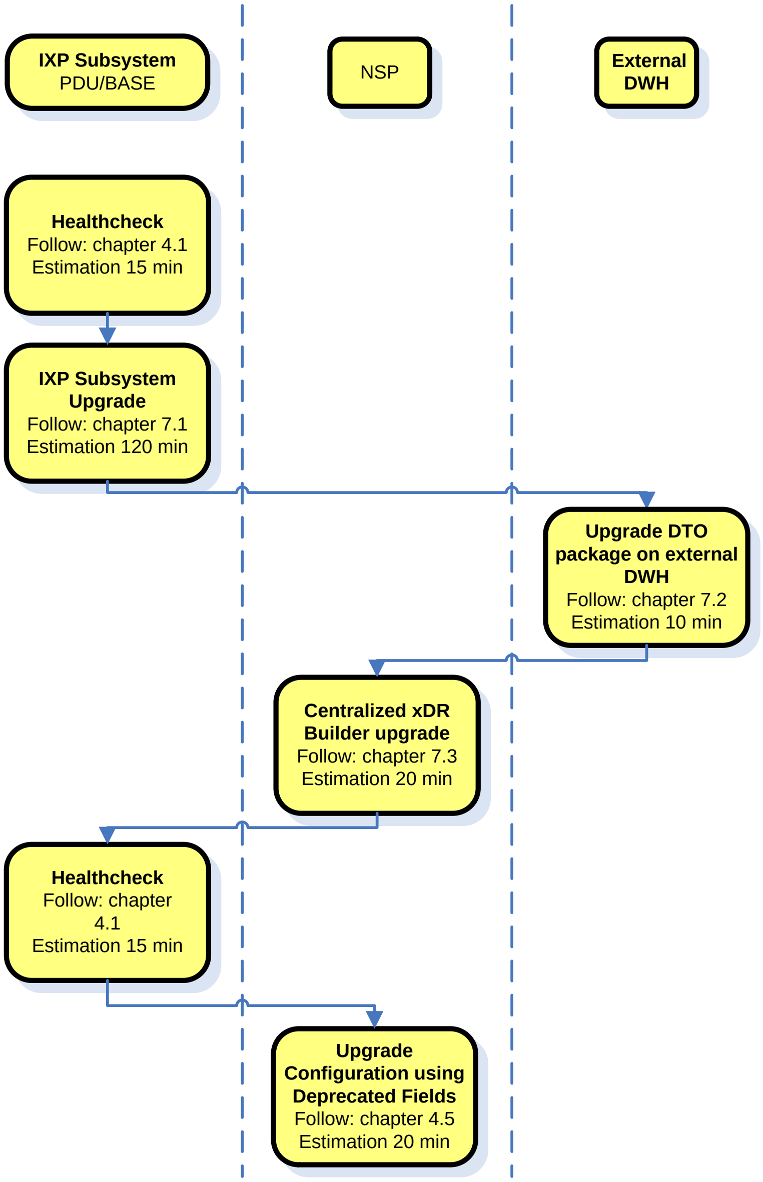
This flowchart depicts the sequence of procedures that must be executed to upgrade the Mediation subsystem and associated server functions.

The Mediation subsystem consists of the following types of servers:

- Mediation PDU storage server
- Mediation Base server

Mediation subsystem incremental upgrade procedure is triggered from one server in the subsystem and 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 Mediation subsystem, all Oracle servers where those sessions are stored must be accessible. Otherwise Centralized xDR Builder upgrade will fail.


IXP Subsystem PDU/BASE
NSP
External DWH
Healthcheck Follow: chapter 4.1 Estimation 15 min
IXP Subsystem Upgrade Follow: chapter 7.1 Estimation 120 min
Upgrade DTO package on external DWH Follow: chapter 7.2 Estimation 10 min
Centralized xDR Builder upgrade Follow: chapter 7.3 Estimation 20 min
Healthcheck Follow: chapter 4.1 Estimation 15 min
Upgrade Configuration using Deprecated Fields Follow: chapter 4.5 Estimation 20 min

Note: Perform 7.4 after Mediation server incremental upgrade is complete and applications have been synced to management server.

3 Incremental Back out Overview Flowcharts

The **back out is** design to come back to the previous release and is applicable **only in case of successful upgrade**. The back out sequence would be similar to the upgrade sequence starting with NSP, then XMF, and Mediation.

3.1 NSP Incremental Back out

NSP application incremental back out is implemented as a Disaster Recovery procedure. Follow the NSP Disaster Recovery Procedure, described in the PIC 10.1.5 Maintenance Guide.

3.2 Acquisition Incremental Back out

Acquisition application incremental back out is implemented as a Disaster Recovery procedure. Follow the Acquisition Disaster Recovery Procedure, described in the PIC 10.1.5 Maintenance Guide.

3.3 Mediation Incremental Back out

Mediation application incremental back out is implemented as a Disaster Recovery procedure. Follow the Mediation Disaster Recovery Procedure, described in the PIC 10.1.5 Maintenance Guide.

4 PIC Health check

4.1 Mediation Subsystem Health check

This procedure describes how to run the automatic health check of the Mediation subsystem.

1. Open a terminal window and log in on any Mediation server in the Mediation subsystem (but not a DWS server) you want to analyze.

2. As `cfguser`, run:

```
$ analyze_subsystem.sh
```

The script gathers the health check 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
```

Note: if you get the error bellow you may use the WA of PR 222200 in order to increase the 80 threshold to 85 for the system having been installed originally with old TPD releases and the / partition is only 500M instead of the 1G allocated on the fresh installed system

```
# syscheck
Running modules in class net...
OK

Running modules in class hardware...
OK

Running modules in class disk...
* fs: FAILURE:: MINOR::5000000000000001 -- Server Disk Space Shortage Warning
* fs: FAILURE:: Space used in "/" exceeds the recommended limit 80%. 84 % used.

# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root
                      496M  398M   73M  85% /
```

Log on the server as root and get the current config:

```
# syscheckAdm --get disk fs
FS_MOUNT_LIST=/, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000,      /boot, -, -, 80, 5000000000000001,
90, 3000000000001000, 80, 5000000000000001, 90, 3000000000001000,      /usr, -, -,
80, 5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000,      /var, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000,      /var/TKLC, -, -, 80,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000,      /tmp, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000
```

Then set the new warning threshold value for "/" directory to 85, replace the first "80" in the value string following "/, -, -, " (note you have to copy all the variable value above and paste it between single quotes):

```
# syscheckAdm --set disk fs --var='FS_MOUNT_LIST' --val='/, -, -, 85,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000,      /boot, -, -, 80, 5000000000000001, 90, 3000000000001000,
80, 5000000000000001, 90, 3000000000001000,      /usr, -, -, 80, 5000000000000001,
90, 3000000000001000, 80, 5000000000000001, 90, 3000000000001000,      /var, -, -,
80, 5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000,      /var/TKLC, -, -, 80, 5000000000000001, 90,
3000000000001000, 80, 5000000000000001, 90, 3000000000001000,      /tmp, -, -, 80,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000'
```

3. Remove back out file
   a) Login as root user on each server
   b) Execute the command to check if the back out file exists
   ```
   # ls /var/TKLC/run/backout
   ```
   c) If the above command returns a result, run the below command to delete the file
   ```
   # rm /var/TKLC/run/backout
   ```

4.2 Acquisition Health check

This procedure describes how to run the health check script on Acquisition servers.
The script gathers the health check information from each server in the Acquisition 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. Run analyze_subsystem.sh script as cfguser:
   ```
   $ analyze_subsystem.sh
   ```
2. 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 Support, Appendix B My Oracle Support (MOS)

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!
```

Note: if you get the error bellow you may use the WA of PR 222200 in order to increase the 80 threshold to 85 for the system having been installed originally with old TPD releases and the / partition is only 500M instead of the 1G allocated on the fresh installed system

```
# syscheck
Running modules in class net...
OK

Running modules in class hardware...
OK

Running modules in class disk...
* fs: FAILURE:: MINOR::5000000000000001 -- Server Disk Space Shortage Warning
* fs: FAILURE:: Space used in "/" exceeds the recommended limit 80%. 84 % used.

# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root
                      496M  398M   73M  85% /
```

Log on the server as root and get the current config:

```
# syscheckAdm --get disk fs
FS_MOUNT_LIST=/, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000,      /boot, -, -, 80, 5000000000000001,
90, 3000000000001000, 80, 5000000000000001, 90, 3000000000001000,      /usr, -, -,
80, 5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000,      /var, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000,      /var/TKLC, -, -, 80,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000,      /tmp, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000
```

Then set the new warning threshold value for "/" directory to 85, replace the first "80" in the value string following "/, -, -, " (note you have to copy all the variable value above and paste it between single quotes):

```
# syscheckAdm --set disk fs --var='FS_MOUNT_LIST' --val='/, -, -, 85,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000,      /boot, -, -, 80, 5000000000000001, 90, 3000000000001000,
80, 5000000000000001, 90, 3000000000001000,      /usr, -, -, 80, 5000000000000001,
90, 3000000000001000, 80, 5000000000000001, 90, 3000000000001000,      /var, -, -,
80, 5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000,      /var/TKLC, -, -, 80, 5000000000000001, 90,
3000000000001000, 80, 5000000000000001, 90, 3000000000001000,      /tmp, -, -, 80,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000'
```

4.3 NSP Pre-Upgrade Health check and Settings

4.3.1 Pre-upgrade Health Check for NSP One-box and Four-box

This procedure describes pre-upgrade sanity test NSP together with a few configuration settings.

1. **Mount PM&C repository**
   Note: This step has to be followed only for c-class blades
   NSP ISO must be mounted on NSP server Refer *How To Mount the ISO file from PM&C ISO Repository*.

2. **Log in and distribute the NSP ISO file**
   a) Login as root user on the NSP server (In case of One-box configuration) or Primary Weblogic server (In case of Four-box configuration).
   b) Copy the NSP ISO on server.

3. **On each HP based management server permit root ssh login.**
   a) As `root` run:

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

4. **Mount the media**
   As `root`, to mount the ISO file, run:

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

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

5. **Pre-Upgrade Verification**
   a) Run health check:

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

   b) The logs are available at `/var/log/nsp/install/nsp_install.log`
   Note: take care the logs keep the history from all previous installation, so make sure to start from the end of the file.
   c) Check the message on terminal console.
   d) If Connection for weblogic User is [NOT OK]. Please Change the weblogic User Password to Default Password.
   Steps to change Weblogic Password

   I. Login as a root user on Primary Weblogic box
   II. Enter platcfg menu:

```
# su - platcfg
```

   III. Navigate to **NSP configuration ⊙ NSP Password Configuration ⊙ Weblogic Password Configuration**
   Note: Under NSP Password Configuration menu there are two submenus

   - NSP Password Configuration (for update/upgrade)
   - Weblogic Password Configuration (for startup and deploy)

   Note: To change the weblogic password during upgrade, second option must be used.
   IV. Change the weblogic password to the default value defined in TR006061 for “Weblogic console”.
   Note: The password must be set to the default value, otherwise upgrade will fail.
   Note: This step can take a while to complete. Wait for Platcfg menu to return back and do not run any outside procedure in between.
   V. Exit platcfg menu.
   Verification of successful password change

   I. Using browser open the URL *http://192.168.1.1/console*, where 192.168.1.1 is the IP address of Apache (In case of Four-box setup) or one-box server (In case of One-box setup)
   II. Enter the new Weblogic password to login to console.
   III. If login is successful, weblogic password has been updated successfully.

IV. If login is unsuccessful, please contact Oracle Support Appendix B My Oracle Support (MOS) and do not proceed with upgrade.

e) If Connection for tekelec User is [NOT OK]. Please Change the tekelec User Password to Default Password.
Steps to change tekelec user Password

I. Connect to Weblogic console.
http://192.168.1.1:8001/console
where **192.168.1.1** is the IP address of NSP server (In case of One-box configuration) or Weblogic Primary Server (In case of Four-box configuration)
II. Login with User name weblogic
III. Click on **Security Realms** in left panel of console window
IV. Click on **myrealm** in right Panel of console window.
V. Click on **Users& Groups** Tab
VI. Click on **users** Tab.
VII. Select **tekelec** user.
VIII. Select **Password** Tab
IX. Change the password to Default Password

Note: If password of tekelec user is not set to default prior to upgrade then upgrade might fail

f) If Connection for TklcSrv User is [NOT OK]. Please Change the TklcSrv User Password to Default Password.
Steps to change TklcSrv user Password

I. Connect to Weblogic console.
http://192.168.1.1:8001/console
where **192.168.1.1** is the IP address of NSP server (In case of One-box configuration) or Weblogic Primary Server (In case of Four-box configuration)
II. Login with User name weblogic
III. Click on **Security Realms** in left panel of console window
IV. Click on **myrealm** in right Panel of console window.
V. Click on **Users& Groups** Tab
VI. Click on **users** Tab.
VII. Select **TklcSrv** user.
VIII. Select **Password** Tab
IX. Change the password to Default Password

Note: If password of TklcSrv user is not set to default prior to upgrade then upgrade might fail

g) **Verify State** and **Health** should be **RUNNING** and **OK** for all three servers (In case of One-box configuration) or All five servers (In case of Four-box configuration).
h) Verify the build number should be 10.x.x-X.Y.Z where X.Y.Z is the build number.
i) Verify the RAM Size is [OK]
j) Verify the space in `/opt`, `/tmp`, `/var/TKLC` is [OK]:

- If you have the message "`space in /var/TKLC is [NOT OK]`" make sure you have only one ISO file in `/var/TKLC/upgrade`. If not, remove all other files; they must be used one by one and not copied all at the same time because the partition is too small.
- If you still have space issue erase the content of the directory `/var/TKLC/backout/pkg` but not the directory itself.
- If the space is still [NOT OK] in any of the above partition, execute the following command to create some default space. Run:

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

  type `yes` to continue.

Please follow step 3(a) again to verify if the space is [OK].

Note: Please do not proceed if space is shown [NOT OK] in any of the above partition. Contact Oracle Support Appendix B My Oracle Support (MOS) and ask for assistance.

k) Verify the free space in `/`, `/opt/oracle` is [OK].
If the space is [NOT OK] in any of the above partition contact Oracle Support Appendix B My Oracle Support (MOS) and ask for assistance.

l) Verify `/tekelec` symlink is present [OK].
If `/tekelec` symlink is not present contact Oracle Support Appendix B My Oracle Support (MOS) and ask for assistance.

m) As `root`, unmounts the ISO file:

```
# umount /mnt/upgrade
```

6. **Verify the free space in vg-root-plat_oracle partition**

a) Login to NSP one box or oracle box in case of 4 box system as root user and execute the below command to know the size of `vg-root-plat_oracle` partition

```
# df -kh
Filesystem                          Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_oracle      7.9G  4.5G  3.1G  60% /usr/TKLC/oracle11
```

If the use% is 90% or above then perform below step to free some space.

b) Move the logs from `vg-root-plat_oracle` partition to `vgroot-plat_nsp` partition as this partition has enough space by performing below steps.

```
# mkdir /usr/TKLC/nsp/alertlogs_backup
# mv /opt/oracle11/oracle/diag/rdbms/nsp_01/NSP/alert /log_*.xml
 /usr/TKLC/nsp/alertlogs_backup
```

If the enough space does not get free by doing above step contact Oracle Support Appendix B My Oracle Support (MOS) and ask for assistance.

7. **Check Weblogic console is not locked**

WARNING

Weblogic console must not be locked during upgrade. If console is locked upgrade will abort. If it is locked, please release lock from Weblogic console as follows:

a) Connect to Weblogic console.
http://192.168.1.1:8001/console
where 192.168.1.1 is the IP address of NSP server (In case of One-box configuration) or Weblogic Primary Server (In case of Four-box configuration).

b) On the left panel click on **Release configuration** button.

8. **Remove backout file**

a) Login as root user on each box of Four-box configuration or on NSP Server if one-box configuration

b) Execute the command to check if the backout file exists

```
# ls /var/TKLC/run/backout
```

c) If the above command returns a result, run the below command to delete the file

```
# rm /var/TKLC/run/backout
```

9. **Check the pkg directory exist**

a) Login as root user on each box of Four-box configuration or on NSP Server if one-box configuration.

b) Execute the command to check if the backout file exists

```
# ls /var/TKLC/backout/pkg
```

c) If the above command does not returns a result, run the below command to create the directory

```
# mkdir /var/TKLC/backout/pkg
```

4.3.2 Pre-upgrade health check for Management Server on ODA

1. **Pre-Upgrade Verification**

a) Please verify the system User Password is Default Password.

b) Please Change the tekelec User Password to Default Password.
Steps to change tekelec user Password

I. Connect to Weblogic console.
http://192.168.1.1:8001/console
where **192.168.1.1** is the IP address of NSP server
II. Login with User name weblogic
III. Click on **Security Realms** in left panel of console window
IV. Click on **myrealm** in right Panel of console window.
V. Click on **Users& Groups** Tab
VI. Click on **users** Tab.
VII. Select **tekelec** user.
VIII.Select **Password** Tab
IX. Change the password to Default Password

Note: If password of tekelec user is not set to default prior to upgrade then upgrade might fail

c) Please Change the TklcSrv User Password to Default Password.
Steps to change TklcSrv user Password

I. Connect to Weblogic console.
http://192.168.1.1:8001/console
where **192.168.1.1** is the IP address of NSP server
II. Login with User name weblogic
III. Click on **Security Realms** in left panel of console window
IV. Click on **myrealm** in right Panel of console window.
V. Click on **Users& Groups** Tab
VI. Click on **users** Tab.
VII. Select **TklcSrv** user.
VIII.Select **Password** Tab
IX. Change the password to Default Password

Note: If password of TklcSrv user is not set to default prior to upgrade then upgrade might fail

d) Verify State and Health should be RUNNING and OK for all three servers
e) Verify the build number should be 10.x.x-X.Y.Z where X.Y.Z is the build number

2. **Check Weblogic console is not locked**

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.
You can find detailed information on the backup in PIC 10.1.5 Maintenance Guide [3], NSP Backup Procedures.

1. Login as a `root` user on NSP Server (In case of One-box configuration) or Oracle server (In case of four-box or ODA configuration).

2. Check the content of /opt/oracle/backup
There must be one directory for the last seven days and it is recommended to copy in a safe place the full content of at least the last of this directory:

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

3. Check the content of the last backup directory

a) 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 PMF_pmf-9010.tgz
```

a) For a Four-box and ODA:

```
# cd NSP_BACKUP_07_04_12_22_00_01
# ls -lh
total 40K
drwxr-xr-x  2 root root 4.0K Jul  4 22:02 apache
-rwxr-xr-x  1 root root  187 Jul  4 22:01 boot.properties
drwxr-xr-x 10 root root 4.0K Jul  4 22:01 config
drwxrwxrwx  2 root root 4.0K Jul  4 22:01 exportrealm
-rw-r--r--  1 root root  376 Jul  4 22:01 failedconnection.txt
-rw-r--r--  1 root root 2.7K Jul  4 22:01 hosts.csv
drwxrwxrwx  2 root root 4.0K Jul  4 12:35 IXP
drwxr-xr-x  7 root root 4.0K Jul  4 22:01 ldap
drwxrwxrwx  2 root root 4.0K Jul  4 22:02 oracle
-rw-r--r--  1 root root  320 Jul  4 22:01 preBackupTests.log
drwxr-xr-x  2 root root 4.0K Jul  4 22:02 primary
drwxr-xr-x  2 root root 4.0K Jul  4 22:02 secondary
-rwxr-xr-x  1 root root   64 Jul  4 22:01 SerializedSystemIni.dat
drwxrwxrwx  2 root root 4.0K Jul  4 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 56M
-rw-r----- 1 oracle oinstall 5.9M Jul  4 22:02 ExpNSP.dmp.gz
-rw-r--r-- 1 oracle oinstall  55K Jul  4 22:02 ExpNSP.log
-rw-r--r-- 1 root   root      371 Jul  4 22:02 hosts
-rw-r--r-- 1 root   root      163 Jul  4 22:02 ifcfg-bond0.3
-rw-r--r-- 1 root   root       99 Jul  4 22:02 ifcfg-eth02
-rw-r--r-- 1 root   root      39K Jul  4 22:02 install.log
-rw-r--r-- 1 root   root      50M Jul  4 22:02 jmxagentproperties.tgz
-rw-r--r-- 1 root   root       76 Jul  4 22:02 network
-rw-r--r-- 1 root   root       62 Jul  4 22:02 nsp_setenv.sh
-rw-r--r-- 1 root   root     1.6K Jul  4 22:02 ntp.conf
-rw-r--r-- 1 root   root     2.5K Jul  4 22:02 snmpd.conf
```

Check the contents of IXP folder. It will be similar to the one below.

```
# ls -lh
total 12K
-rwxr-x--- 1 oracle oinstall 610 Apr  7 09:05 IXP_ixp1000-1a.tgz
-rwxr-x--- 1 oracle oinstall 645 Apr  7 09:05 IXP_ixp1000-1b.tgz
-rwxr-x--- 1 oracle oinstall 560 Apr  7 09:05 IXP_ixp1000-1z.tgz
```

Check the contents of XMF folder. It will be similar to the one below.

```
# ls -lh
total 4.0K
-rwxr-x--- 1 oracle oinstall 296 Apr  7 09:05 XMF_pmf-9010.tgz
```

Note: the backup is automatically executed each night at 22H00 and depending on the time you start NSP upgrade you may execute a manual backup just before to start the upgrade.

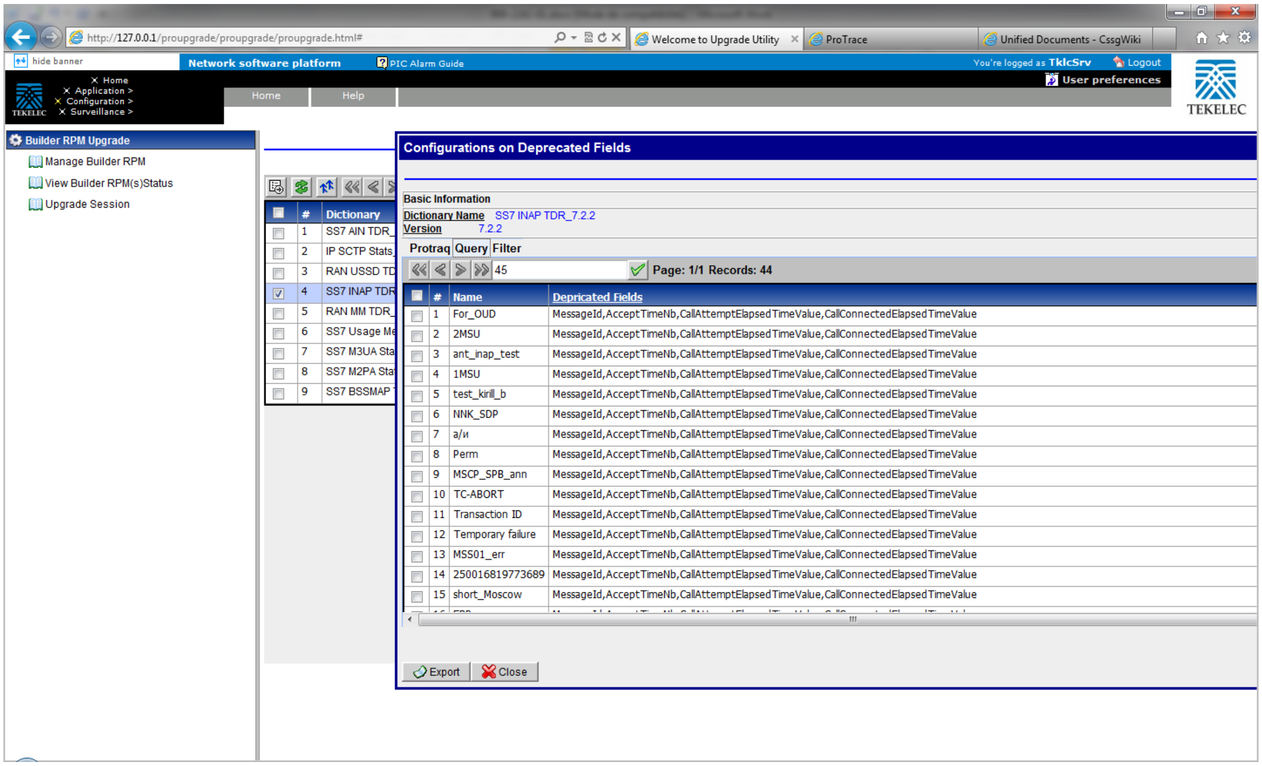
4.5 Upgrade Configurations using Deprecated Field(s)

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.

1. Login to NSP application interface as TklcSrv user.
2. Click **Upgrade Utility**
3. Click **Dictionaries with Deprecated Field(s)** link on home page, this will a list of dictionaries having deprecated field(s).
4. Select any one of the dictionaries and choose **View Dependent 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 dependent configurations then this list will be empty.

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

4.6 Global Health check

4.6.1 iLO Access

Make sure you can access the iLO interface of all servers and you can open the remote console for each server.

4.6.2 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.

4.6.3 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

4.6.4 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. Obtain session period and time (clock icon)
3. Filter by end date
4. End date must be the correct time
5. 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.

4.6.5 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.

4.6.6 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.

4.6.7 ProTraq

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

4.6.8 ProPerf

Access to ProPerf configuration and check each dashboard is working fine

4.6.9 DataFeed

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

4.6.10 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.

4.6.11 Capacity Management

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 Incremental Upgrade

5.1 NSP Pre-Upgrade Check (one-box and four-box)

Note: Please proceed on this procedure for ODA from 2 f) onwards.

1. **Make sure you executed the sections:**
   a) NSP Pre-Upgrade Health check and settings
   b) Upgrade configuration using deprecated fields
   c) Check NSP Backup is Valid

2. **Pause JMS and Purge terminated alarm**
   This procedure does the following tasks:
   - a. Pauses JMS consumption
   - b. Purges Alarm
   - c. Corrects /tekelec symlink path
   - d. Reconfigures Enterprise manager if it is not correctly configured

   a) Login as root user on NSP Server In case of One-box configuration) or Primary weblogic server (In case of Four-box configuration).

   b) Execute the following command to mount Management ISO:

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

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

   c) Run pre-upgrade config:

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

   Note: If you get the message below just answer “y” in order to unlock weblogic console

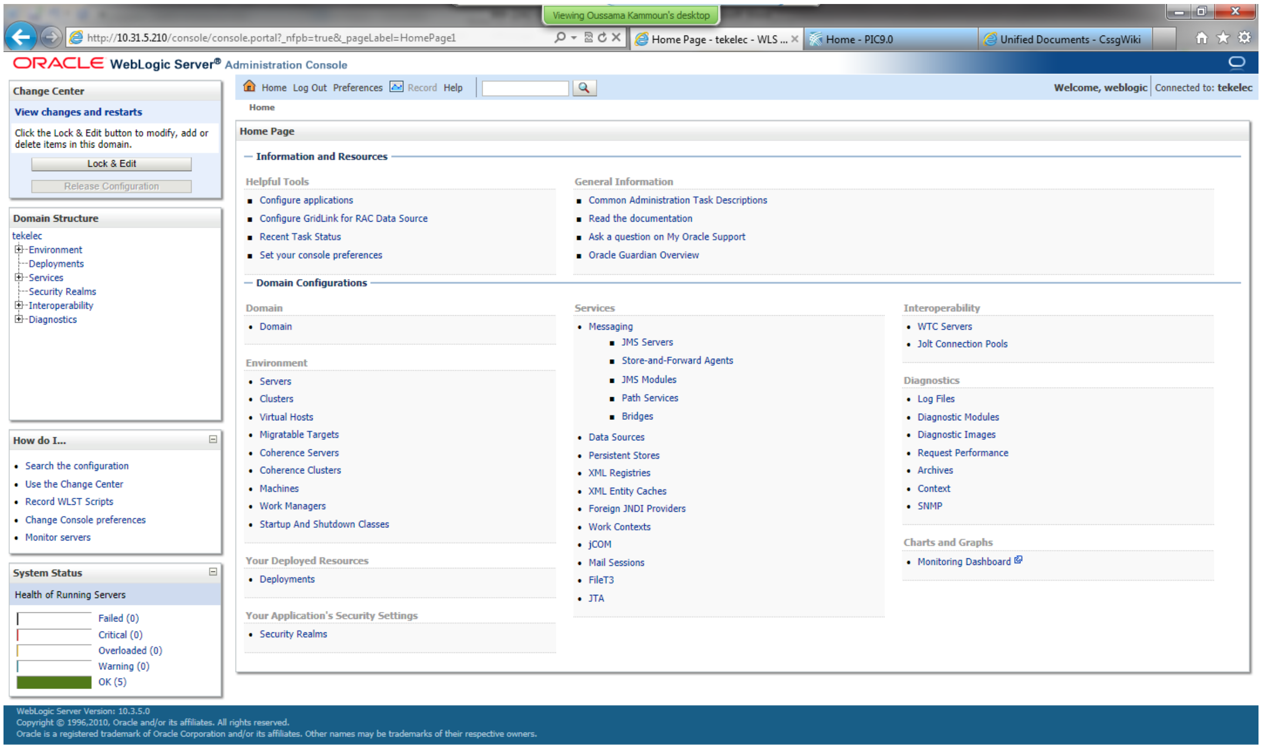
   ```
   *****************  Purge Terminated Alarms  *********************************
   Purging Terminated Alarms
   Number of Terminated Alarms: 92456
   Number of All Alarms: 92639
   Do you want to purge Alarms prior to backing up oracle db [y/n]?
   ```

   d) Type “y” to continue for purging of terminated alarms.
   To purge terminated Alarms `enter 1` or to purge All Alarms `enter 2`

   e) Unmount Management Server ISO

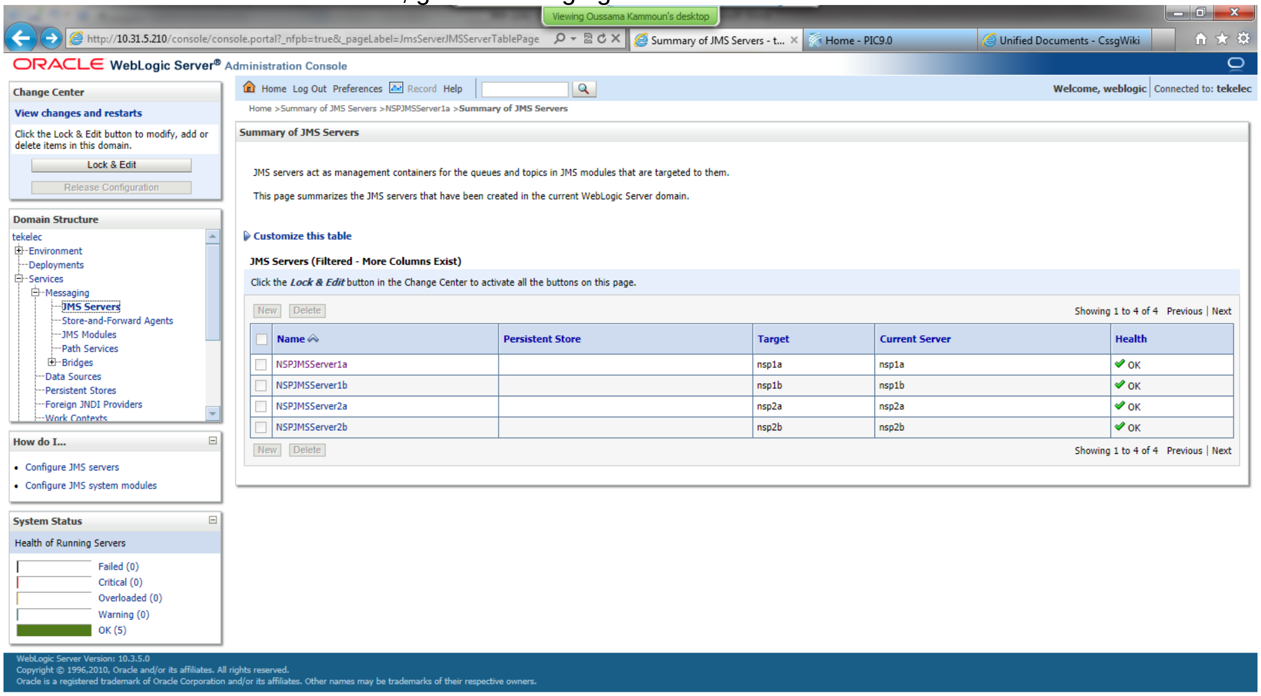
   ```
   # umount /mnt/upgrade
   ```

   f) Connect to Weblogic console in order to check JMS consumption is really stopped.



WebLogic Server Version: 10.3.5.0
Copyright © 1996,2010, 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.

In the Services section, go to messaging and then JMS Servers menu:


Viewing Oussama Kammoun's desktop
http://10.31.5.210/console/console.portal?_nfpb=true&_pageLabel=JmsServerJMSServerTablePage
Summary of JMS Servers - t...
Home - PIC9.0
Unified Documents - CssgWiki
ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: tekelec
Home >Summary of JMS Servers >NSPJMSServer1a >Summary of JMS Servers
Change Center
View changes and restarts
Click the Lock & Edit button to modify, add or delete items in this domain.
Lock & Edit
Release Configuration
Domain Structure
tekelec
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
Work Contexts
How do I...
Configure JMS servers
Configure JMS system modules
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (5)
Customize this table
New
Delete
Showing 1 to 4 of 4 Previous | Next

Summary of JMS Servers

JMS servers act as management containers for the queues and topics in JMS modules that are targeted to them.

This page summarizes the JMS servers that have been created in the current WebLogic Server domain.

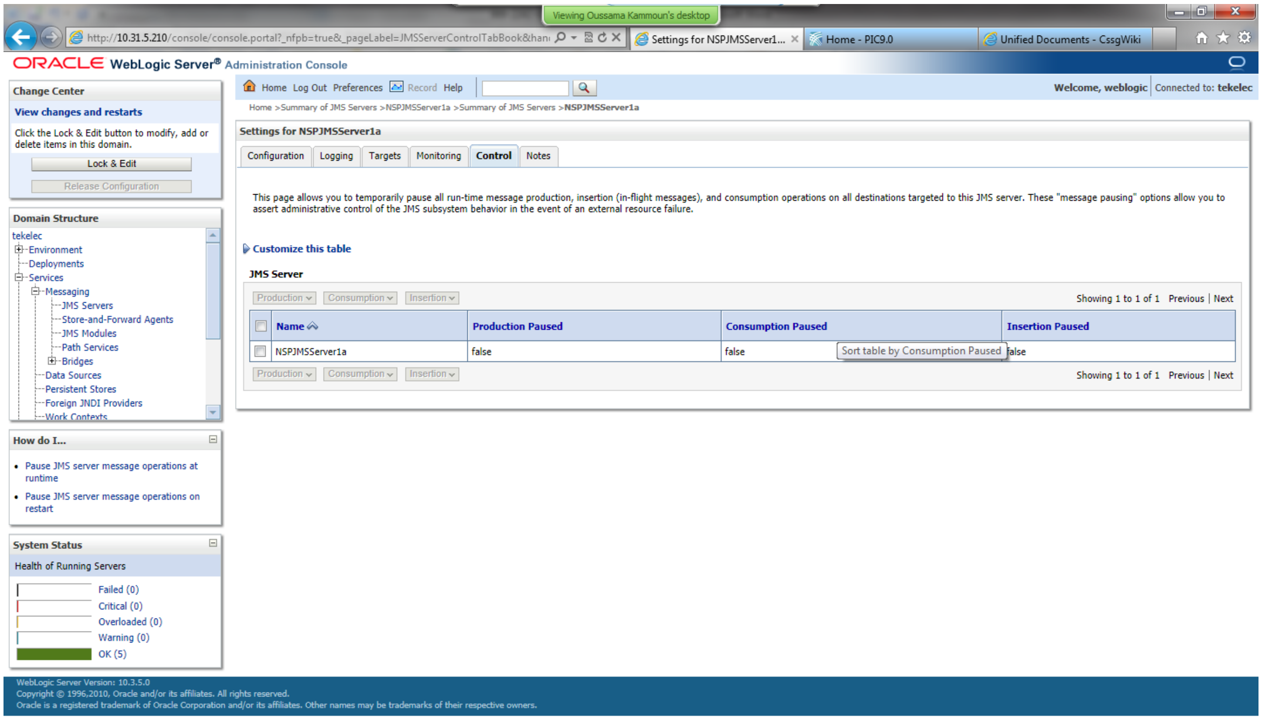
JMS Servers (Filtered - More Columns Exist)

Click the *Lock & Edit* button in the Change Center to activate all the buttons on this page.

□	Name	Persistent Store	Target	Current Server	Health
□	NSPJMSServer1a		nsp1a	nsp1a	✓ OK
□	NSPJMSServer1b		nsp1b	nsp1b	✓ OK
□	NSPJMSServer2a		nsp2a	nsp2a	✓ OK
□	NSPJMSServer2b		nsp2b	nsp2b	✓ OK

WebLogic Server Version: 10.3.5.0
Copyright © 1996,2010, 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.

For Each JMS servers (2 in case on One-box or ODA, and 4 if it is a Four-box), click on the name of the server and then to the menu Control:


Viewing Oussama Kammoun's desktop
http://10.31.5.210/console/console.portal?_nfpb=true&_pageLabel=JMSServerControlTabBook&han
Settings for NSPJMSServer1...
Home - PIC9.0
Unified Documents - CssgWiki
ORACLE WebLogic Server® Administration Console
Change Center
View changes and restarts
Click the Lock & Edit button to modify, add or delete items in this domain.
Lock & Edit
Release Configuration
Domain Structure
tekelec
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
Work Contexts
How do I...
Pause JMS server message operations at runtime
Pause JMS server message operations on restart
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (5)
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: tekelec
Home >Summary of JMS Servers >NSPJMSServer1a >Summary of JMS Servers >NSPJMSServer1a
Configuration
Logging
Targets
Monitoring
Control
Notes
Customize this table
Production
Consumption
Insertion
Showing 1 to 1 of 1 Previous | Next
Sort table by Consumption Paused

Settings for NSPJMSServer1a

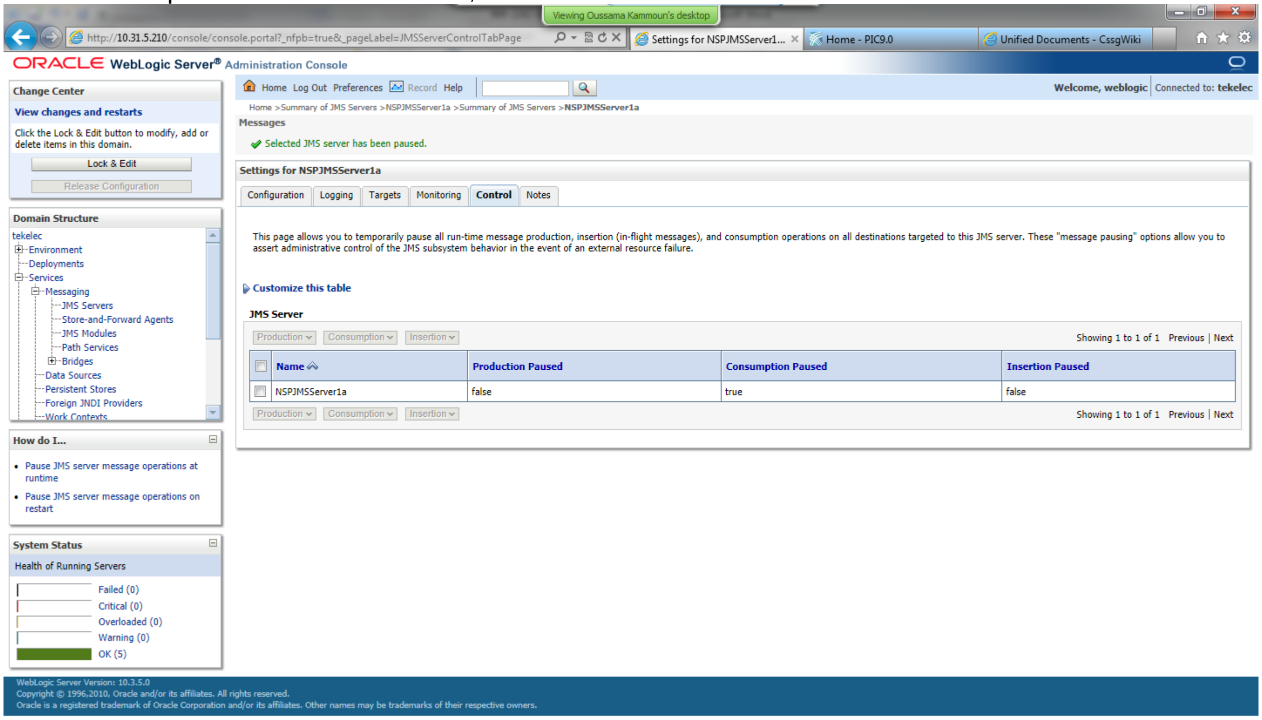
This page allows you to temporarily pause all run-time message production, insertion (in-flight messages), and consumption operations on all destinations targeted to this JMS server. These "message pausing" options allow you to assert administrative control of the JMS subsystem behavior in the event of an external resource failure.

JMS Server

□	Name	Production Paused	Consumption Paused	Insertion Paused
□	NSPJMSServer1a	false	false	false

WebLogic Server Version: 10.3.5.0
Copyright © 1996,2010, 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.

If the value in consumption paused is true, this server is paused and you can return to previous step in order to check the status of the next JMS server.
If the value is false like of the screenshot, select the checkbox in order to activate the menu consumption, and then select pause. When asked to confirm if you Are sure you want to pause consumption for this JMS server?, answer Yes.


Viewing Oussama Kammoun's desktop
http://10.31.5.210/console/console.portal?_nfpb=true&_pageLabel=JMSServerControlTabPage
Settings for NSPJMSServer1...
Home - PIC9.0
Unified Documents - CssgWiki
ORACLE WebLogic Server® Administration Console
Change Center
View changes and restarts
Click the Lock & Edit button to modify, add or delete items in this domain.
Lock & Edit
Release Configuration
Domain Structure
tekelec
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
Work Contexts
How do I...
Pause JMS server message operations at runtime
Pause JMS server message operations on restart
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (5)
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: tekelec
Home >Summary of JMS Servers >NSPJMSServer1a >Summary of JMS Servers >NSPJMSServer1a
Configuration
Logging
Targets
Monitoring
Control
Notes
Customize this table
Production
Consumption
Insertion
Showing 1 to 1 of 1 Previous | Next

Messages

✓ Selected JMS server has been paused.

Settings for NSPJMSServer1a

This page allows you to temporarily pause all run-time message production, insertion (in-flight messages), and consumption operations on all destinations targeted to this JMS server. These "message pausing" options allow you to assert administrative control of the JMS subsystem behavior in the event of an external resource failure.

JMS Server

□	Name	Production Paused	Consumption Paused	Insertion Paused
□	NSPJMSServer1a	false	true	false

WebLogic Server Version: 10.3.5.0
Copyright © 1996,2010, 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.

The value in consumption paused is true now as expected, so you can return to the JMS server list in order to check the status of the next one, or continue next step if this was the last one.

3. **Check minimum free disk space in /usr/TKLC/oracle/backup**
   Note: This step needs to be followed on NSP One-box or Oracle Server only and **not for ODA**.
   a) As root run:

```
# df -kh /usr/TKLC/oracle/backup
```

   Example output:

```
Filesystem          Size   Used   Avail   Use%   Mounted on
/dev/cciss/c0d2p1   67G    11G    57G     16%   /usr/TKLC/oracle/backup
```

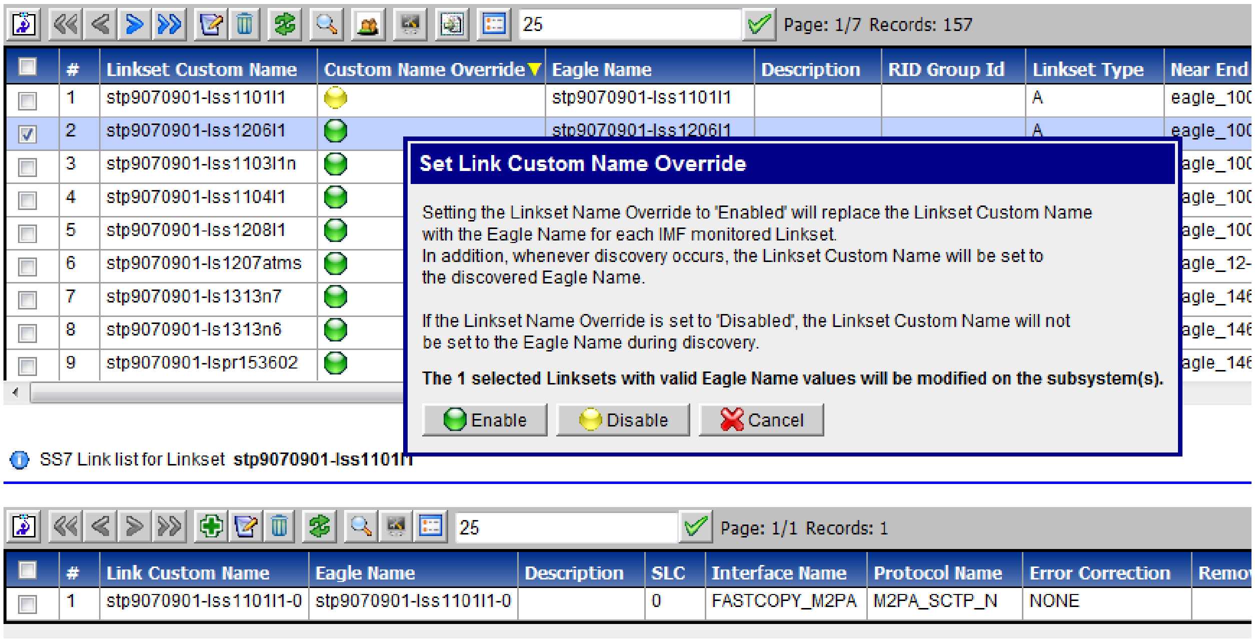
   b) Check the space available under Avail column of this table. This should be at least 15-20 GB approx. e.g. in above table shown total space available is 57GB.
   Note: If total available space is less than 2 GB, then do not continue with upgrade. Contact Oracle Support Appendix B My Oracle Support (MOS) and ask for assistance.

4. **Generate the “Bulk Export Configurations” and “Create Configuration Report”**
   Go to the CCM home page and click on the link to generate this files.
   Keep it in a safe place on your laptop in the worst case where even a disaster recovery would not work with would help you to get in information, in order to re-create the configuration.

5. **Synchronize the Integrated Acquisition**
   Go to the CCM and synchronize the Integrated Acquisition in the acquisition part before to start any operation in order to avoid discovering new links while the upgrade.

   WARNING

   Take care if the Custom Name Override feature is enable on the link set, the names would be replaced by the one used on the Eagle.
   The function is available on the Linksets list page tool bar.



25 ✓ Page: 1/7 Records: 157

☐	#	Linkset Custom Name	Custom Name Override	Eagle Name	Description	RID Group Id	Linkset Type	Near End
☐	1	stp9070901-lss1101l1	●	stp9070901-lss1101l1			A	eagle_10
☑	2	stp9070901-lss1206l1	●	stp9070901-lss1206l1			A	eagle_10
☐	3	stp9070901-lss1103l1n	●					agle_10
☐	4	stp9070901-lss1104l1	●					agle_10
☐	5	stp9070901-lss1208l1	●					agle_10
☐	6	stp9070901-ls1207atms	●					agle_12-
☐	7	stp9070901-ls1313n7	●					agle_14
☐	8	stp9070901-ls1313n6	●					agle_14
☐	9	stp9070901-lspr153602	●					agle_14

Set Link Custom Name Override

Setting the Linkset Name Override to 'Enabled' will replace the Linkset Custom Name with the Eagle Name for each IMF monitored Linkset.
In addition, whenever discovery occurs, the Linkset Custom Name will be set to the discovered Eagle Name.

If the Linkset Name Override is set to 'Disabled', the Linkset Custom Name will not be set to the Eagle Name during discovery.

The 1 selected Linksets with valid Eagle Name values will be modified on the subsystem(s).

SS7 Link list for Linkset **stp9070901-lss1101l1**

25 ✓ Page: 1/1 Records: 1

☐	#	Link Custom Name	Eagle Name	Description	SLC	Interface Name	Protocol Name	Error Correction	Remo
☐	1	stp9070901-lss1101l1-0	stp9070901-lss1101l1-0		0	FASTCOPY_M2PA	M2PA_SCTP_N	NONE	

5.2 *Incremental Upgrade Apache (four-box only)*

Warning: This step is applicable to four-box configuration only. Skip it for one-box config and ODA.
Box: Apache box

1. **Mount PM&C repository**
   Note: This step has to be followed only for c-class blades
   NSP ISO must be mounted on NSP server. Refer *How To Mount the ISO file from PM&C ISO Repository*.

2. **Upgrade Apache Box**
   a) Login as root user on the Apache Box.
   b) Copy the NSP Software ISO at path `/var/TKLC/upgrade`

Note: Step (b) is only applicable for rack mount servers.

c) Mount the ISO file

```
# 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).

d) As root, run:

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

```
# /mnt/upgrade/upgrade_nsp.sh
```

Where /mnt/upgrade is the mount point where NSP iso is mounted

e) 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.

f) 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 ***Error! Reference source not found.***

5.3 Incremental Upgrade Oracle (four-box only)

Warning: This step is applicable to four-box configuration only. Skip it for one-box config and ODA
Box: Oracle box

1. **Mount PM&C repository**
   Note: This step has to be followed only for c-class blades
   NSP ISO must be mounted on NSP server. Refer *How To Mount the ISO file from PM&C ISO Repository*.

2. **Upgrade Oracle Box**
   a) Login as root user on the Oracle Box.
   b) Copy the NSP Software ISO at path `/var/TKLC/upgrade`
   Note: Step (b) is only applicable for rack mount servers
   c) Mount the ISO file

```
# 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).

c) As root, run:

Note: Run this procedure via iLO or through any 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.

e) 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.
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` **Error! Reference source not found.**

5.4 Upgrade NSP on Secondary WebLogic (four-box only)

Warning: This step is applicable to four-box configuration only. Skip it for one-box config and ODA

Box: Secondary WebLogic box

1. **Mount PM&C repository**
   Note: This step has to be followed only for c-class blades
   NSP ISO must be mounted on NSP server Refer *How To Mount the ISO file from PM&C ISO Repository*.

2. **Upgrade NSP on Seondary Weblogic Box**
   a) Login as root user on terminal console of NSP secondary weblogic server.
   b) Copy the NSP ISO on server.
   c) Mount the ISO file

   ```
   # 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).
   d) As root, run:
   Note: Run this procedure via iLO or through any disconnectable console only.

   ```
   # /mnt/upgrade/upgrade_nsp.sh
   ```

   Note: /mnt/upgrade is the mount point where NSP ISO is mounted
   e) 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.
   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 **Error! Reference source not found.**

5.5 Upgrade NSP on Primary Weblogic(four-box only)

Box: Primary WebLogic box

1. **Mount PM&C repository**
   Note: This step has to be followed only for c-class blades
   NSP ISO must be mounted on NSP server Refer *How To Mount the ISO file from PM&C ISO Repository*.

2. **Weblogic Installation/Upgrade**
   c) Login as root user on terminal console of Primary Weblogic server.
   d) Copy the NSP ISO on server.
   c) Mount the ISO file

   ```
   # 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).
   d) As root, run:
   Note: Run this procedure via iLO or through any disconnectable console only.

   ```
   # /mnt/upgrade/upgrade_nsp.sh
   ```

   Note: /mnt/upgrade is the mount point where NSP ISO is mounted
   e) 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. 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 **Error! Reference source not found.**

5.6 Upgrade NSP on One-box

Warning: This step is applicable to one-box or ODA .
Box: One-box or ODA Admin Server

1. **Mount PM&C repository**

   Note: This step has to be followed only for c-class blades
   NSP ISO must be mounted on NSP server Refer *How To Mount the ISO file from PM&C ISO Repository*.

2. **Upgrade NSP**

   a) Login as root user on terminal console of NSP server or ODA Admin Server.
   b) Copy the NSP ISO on server.
   c) Mount the ISO file

```
# 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).
   d) As root, run:
   Note: Run this procedure via iLO or through any disconnectable console only.

```
# /mnt/upgrade/upgrade_nsp.sh
```

   Note: /mnt/upgrade is the mount point where NSP ISO is mounted
   Note: The upgrade script will ask for user and IP address information related to ODA. Please provide the same. Refer Section 6.2.2 in **[7]**
   e) 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. 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 **Error! Reference source not found.**

5.7 Post-Upgrade Settings (one-box and four-box)

Warning: This step is applicable to ODA, one-box and four-box configurations.
Box: One-box, ODA or Primary WebLogic boxes.

1. **Resume JMS Consumption**

   Note: This step should be skipped for ODA.

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

b) Execute the command below to resume JMS consumption

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

2. **Configure Apache HTTPS Certificate (Optional)**

   Note: For ODA please refer section **7.4 in [3]**

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

   b) From platcfg root menu navigate to **NSP Configuration ⊙ Configure Apache HTTPS Certificate**
   This would install certificate provided by customer

3. **Restrict access of NSP frontend to HTTPS (Optional)**
   Disable access to HTTP

   Note: For ODA please refer **section 7.14 in [3]**

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

   b) Enter the platcfg 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 (Four-Box)

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

   ```
   # su – platcfg
   ```

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

   h) Select **YES** and press **OK**

4. **NSP Applications Documentation**
   Note: Document for application is automatically installed along with NSP application installation
   To verify document installation login into NSP application interface and navigate to **Help ⊙ User Manual** Index page for that application opens. (Each application should be tested and also the link to the PDF should be tested to see if the printable PDF file opens.)
   In case you have problems to access some applications such ProTrace, ProTraq or CCM try to empty you browser cache.

5. **Configure host file for Mail Server (Optional)**

   Note: For ODA please **refer section 7.8 in [3]**
   Note: This configuration is optional and required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined and no server address override defined by app).
   Note: Apply following steps on Primary server and Secondary server in case of Four-box configuration

   a) Open a terminal window and log in as `root` user on NSP server.

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

   ```
   # su – platcfg
   ```

   c) Navigate to Network **Configuration ⊙ Modify host file ⊙ Edit** and press enter

   d) Select **Add Alias** menu and press enter

   e) Select line with machine `<ip>` and press enter

   f) Enter new alias as `mail.server` in the text field press **OK**

   g) Repetitive exit to exit platcfg menu

6. **Transfer Ownership of TklcSrv object**
   Note: Follow the steps only if some object bellowing to TklcSrv 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)

7. **To enable or disable the legacy feeds refer the PIC 10 Maintenance Guide Error! Reference source not found. when needed. (Optional)**

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

8. **MIB has changed between 9.0 and 10**
   To be provided to customer if needed.

5.8 NSP Post-Upgrade Check (one-box and four-box)

Warning: This step is applicable to ODA, one-box and four-box configurations.
Box: must be done from a workstation browser.
This procedure describes the steps for the Sanity Tests of NSP.
Note: Execute steps 1 to 10 and 13 on ODA

1. **WebLogic Console**
   From Internet Explorer, connect to the WebLogic console using the following URL:
   `http://192.168.1.1:8001/console`
   where **192.168.1.1** is the IP address of the NSP Server (In case of One-box configuration) or WebLogic Primary Server (In case of Four-box configuration).
2. **Login**
   You should be prompted to “Log in to work with the WebLogic Server domain “.
   Connect with User **weblogic**
3. **Console Display**
   Under the **Environment** heading, click on the “**Servers**”.
4. **Health Check**
   a) On clicking the “Servers” link in the last step, the console would display the **Summary of Servers**, with a list of the three servers, nsp1a, nsp1b and nspadmin (In case of One-box configuration) or all five server,nsp1a,nsp1b,nsp2a,nsp2b and nspadmin (In case of Four-box configuration).
   b) Entries in the columns **State** and **Health** should be **RUNNING** and **OK** for all three servers (In case of One-box configuration) or five servers (In case of Four-box configuration).
5. **NSP GUI**
   From Internet Explorer, connect to the NSP Application GUI using the following URL:
   `http://192.168.1.1/`
   where 192.168.1.1 is the IP address of the NSP Server (in case of One-box configuration) or the IP of the Apache server (in case of Four-box configuration).
6. **Login**
   Login to the Application with User name **tekelec**
7. **Portal**
   a) In the top frame, on mouse-over on the link **Portal**, click on the **About** link that will be displayed.
   b) A pop-up window with the build information will be displayed.
8. **Build Verification**
   The build version should display “Portal 9.0.0-X.Y.Z”. Where 9.0.0-X.Y.Z should be the new build number.
9. **Check Oracle Enterprise manger connection**
   a) From Internet Explorer, connect to the following URL:
   `https://192.168.1.1:1158/em/`
   where 192.168.1.1 is the IP of the NSP server (in case of One-box configuration) or the IP of the Oracle server (in case of Four-box configuration).
   b) You should be prompted to log in to work with the Enterprise manager.
   Connect with User **nsp.**
10. **Verify ProTraq Configurations**
    This step is only for Information in order to get the log in case of troubles while the Centralized xDR Builder upgrade. The ProTraq config identified with issues here would be automatically modified while this step.

a) Login to NSP Primary using `tekelec` user

b) Change Directory:

```
$ cd /opt/nsp/nsp-package/protraq
```

c) Execute:

```
$ ant dryrun
```

d) Enter Password for Tekelec Service User(TklcSrv)

e) The target will complete with following output:

i) ProTraq Configurations having Field Value Columns with IP V4 Attribute Type would be displayed under “Following Configurations have Field Value Columns with IP V4 Data Type.”

ii) ProTraq Configurations Field Value Columns with IP V4 Attribute Type with invalid line names would be listed under “Following Configurations have Line Names exceeding permissible length. Please modify the configurations to correct the line names.”

f) Open NSP GUI → ProTraq, Modify ProTraq Configurations listed in step e(ii) to correct the Line Names.

g) Execute ant target again:

```
$ ant dryrun
```

No configurations with invalid line names should be listed now.

Verify ./LineDryRun*.log; there should be no errors.

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

12. 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. However during this step the server will be rebooted. The logs should be verified after the server has come up from reboot.

13. **On each HP based management server revoke root ssh login.**

a) As `root` run:

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

14. 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
```

15. Execute following on ODA only ,as root user on Admin Server of ODA:

```
Execute below command to verify if the rules have been set
# iptables -L -n -t nat -v
Sample output in case of correct port forwarding rules:
[root@WL_tekelec_AS ~]# iptables -L -n -t nat -v
Chain PREROUTING (policy ACCEPT 57376 packets, 2381K bytes)
 pkts bytes target     prot opt in     out     source               destination
  363 21780 DNAT       tcp  --  eth1   *       0.0.0.0/0            10.31.2.82
tcp dpt:7001 to:192.168.16.64:7001

Note: If the rules are not set then execute configureFirewall.sh script to setup
else skip the execution of this script.

# sh /opt/nsp/nsp-
package/framework/install/dist/install/post_installation/configureFirewall.sh
Expected output of the command is mentioned below:
net.ipv4.ip_forward = 1
Saving firewall rules to /etc/sysconfig/iptables:          [  OK  ]
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: nat filter                [  OK  ]
Unloading iptables modules:                                [  OK  ]
Applying iptables firewall rules:                          [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n[  OK  ]


# chmod 700 /opt/nsp/.ssh
# chmod 600 /opt/nsp/.ssh/*
```

5.9 NSP Backup (one-box and four-box)

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

For ODA: Please check if backup Job “NSP_BACKUP_JOB” is running as Oracle scheduled Job.

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 Acquisition and Mediation 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.

Note:This only one command line. You might use the command crontab –l to display the command lanched each night and just copy it.

```
# 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
```

5.10 Upload xDR Builder ISO to NSP (one-box and four-box)

Warning: This step is applicable to one-box , ODA and four-box configurations.
Box: ODA Admin Server, One-box or Primary WebLogic box + workstation browser

This procedure describes how to trigger the xDR builder installation on the Mediation subsystem from the
CCM.
Note 1: In case of failure in this step this is not blocking for the Acquisition upgrade but only for the Mediation. This will give some time to Design Support to investigate the reason of this over the day.
Note 2: PIC supports Mediation subsystems with 32 and 64 bit platform architecture. For an Mediation 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 ODA Admin Server or NSP primary Weblogic server or insert xDR Builder CD-ROM.
   b) Login to the ODA Admin Server or 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) Enter the exact path including the ISO name
   e) Wait until installation finishes.
   Note: The script will ask for root password for many (approximately 5-6 times), please take care to provide the same.

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 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 is using deprecated field and configurations which will become incompatible after removal of field.
If there are configurations (Query/Protraq/xDR filter) on the removed field, then modify those configurations to remove the use of removed field. Otherwise those configurations will be removed from the NSP when you upload the builder RPM.
The dry run can't anymore be executed once the new package would be installed on the Mediation subsystem but you would have access to similar information on the deprecated fields menu you can access from the utility home page.

4. **Upload Builder RPM**

   a) Mark the requested builder RPM with the **Not Uploaded** state and press **Upload** in the toolbar.
   b) A dialog box will appear. Click on Continue to continue the RPM upload.
   c) After the successful upload the RPM state will change to **Uploaded**
   d) In case the RPM upload fails, then the state of will change back to "Not Uploaded" or "Query/Filter Upgrade Failed".

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

5. **Upgrade Queries and Filters**

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

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

6. **View Dictionary Upgrade Status**

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

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

6 Acquisition Incremental Upgrade

6.1 Acquisition Upgrade

1. **Copy ISO image to the server**
   Copy ISO image to the `/var/TKLC/upgrade` directory of the server.

2. **Upgrade the server**
   a) As root on the Acquisition server
   b) Enter platcfg configuration menu
   ```
   # su – platcfg
   ```
   c) Navigate to Maintenance ➤Upgrade
   d) Select Initiate Upgrade
   e) Select the desired upgrade media

Note:

1. Please perform the above steps (for Upgrade) using ILO or any non-disconnectable media.
2. 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.

3. **Upgrade proceeds**
   a) Many informational messages appear on the terminal screen as the upgrade proceeds. To make it easier to read, the messages are not shown here.
   b) When upgrade is complete, the server reboots.

4. **Upgrade completed**
   After the reboot, the screen displays the login prompt.

5. **Check the log**
   a) In platcfg navigate to Diagnostics > View Upgrade Logs > Upgrade Log
   b) Check on the bottom of the file the upgrade is complete

6.2 Sync NSP with Acquisition

1. **Apply Changes Acquisition**

   Note: If the two first digits of Acquisition version has changed during incremental upgrade procedure (e.g.: from 10.0 to 10.1), then it is necessary to perform Discovery procedure: go to **Equipment Registry** ⊙ **Sites** ⊙ **XMF**, select a XMF server and click on **Discover Application** button.

   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.

2. **Test the VIP function.**
   a) After sync from NSP, the VIP will be available to access the active master server in the site. In order to verify the VIP setup please login to any server in the subsystem and execute the `iFoStat` command. As `cfguser` run:
   ```
   $ iFoStat
   ```
   Example of correct output:

```
query 10.236.2.79 for failover status
+---------+-------+-----+-----------+----------+------+---------------------+
| name    | state | loc | role      | mGroup   | assg | HbTime              |
+---------+-------+-----+-----------+----------+------+---------------------+
| tek3-1a | IS    | 1A  | ActMaster | sde_m2pa |    8 | 2009-06-19 23:14:08 |
| tek3-1b | IS    | 1B  | StbMaster | sde_stc  |    6 | 2009-06-19 23:14:06 |
| tek3-1c | IS    | 1C  | Slave     |          |    0 | 2009-06-19 23:14:06 |
+---------+-------+-----+-----------+----------+------+---------------------+
```

b) The state should be ‘IS’ for all servers and the HbTime time should be updated every few seconds.

7 Mediation Incremental Upgrade

7.1 Mediation Subsystem Upgrade

This procedure describes the Mediation application incremental upgrade procedure. Be aware of each step. The Mediation incremental upgrade is executed on each server in the subsystem in parallel. The parallel Mediation subsystem incremental upgrade is triggered from one server in the subsystem; it cannot be triggered more than once per subsystem. The upgrade must be triggered from any connectable medium or using ILO.

1. **Permit root ssh login**

   On each IXP server permit root ssh login.

   b) As `root` run:

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

2. **Distribute the Mediation ISO**

   Note: Choose one of the servers in the subsystem. From this server you will trigger the parallel Mediation subsystem incremental upgrade.

   a) Distribute the Mediation ISO file to `/var/TKLC/upgrade` directory.

      a. On the rack mount server copy the Mediation ISO into the `/var/TKLC/upgrade` using the scp command.

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

3. **Run parallel Mediation subsystem upgrade**

   Note: Run this step on where server where you distributed the Mediation ISO. This step will trigger the parallel incremental upgrade on all servers in the subsystem.

   c) As `root` run:

   ```
   # misc_upgrade_subsystem.sh -i iso_filename
   ```

   where *`iso_filename`* is the name of the Mediation ISO file that has been previously distributed on this server.

   d) You will be prompted to confirm the upgrade; then, you will be asked to enter the root password. The incremental upgrade is triggered on all the servers of the subsystem.

4. **Monitor parallel Mediation incremental upgrade**

   Note: The whole subsystem is upgrading now. Keep logged on the server where you have triggered the parallel upgrade, as you will see the progression. The server will reboot after successful upgrade.

   a) Once the server where you have triggered the parallel upgrade is accessible again, start monitoring script: it will apply some subsystem post-upgrade settings, after all the servers have successfully upgraded (and rebooted). As `root` run:

   ```
   # misc_upgrade_subsystem.sh --postsync
   ```

   b) You will see the regular monitoring of the upgrade progress. Keep this script running and look for successfully upgraded servers. **Do not interrupt** the script. Wait until the results of upgrade are shown and synchronization is restored. Monitor the script output for any errors. The logs for the upgrade must be verified at /var/TKLC/log/upgrade/upgrade.log on the server from where the upgrade is triggered. If any error appears contact Oracle Support Appendix B My Oracle Support (MOS). The script will only finish once all servers in the subsystem have finished the upgrade.

5. **Discover IXP application in CCM**

This procedure describes how to discover Mediation application in the NSP Centralized Configuration application.

Discover all Mediation servers in Centralized Configuration application.

a) Open a web browser and go to the NSP application interface main page.
b) Click **Centralized Configuration**.
c) Navigate to **Equipment registry** view.
d) Open **Sites**, open the site, open **IXP** and then click on the particular Mediation subsystem.
e) The list of all Mediation servers in the Mediation subsystem will appear. Check the check box of the first server and click the **Discover Applications** button. Wait until the IXP application will be discovered. Then repeat this step for all servers in the subsystem.
f) Navigate to Mediation and Apply the changes on the Mediation subsystem.

6. **Generate the bulkconfig file for the Mediation subsystem**

Note: For a future use generate the `bulkconfig` file from the subsystem settings. The file is generated on a single server and then automatically distributed to all servers in the subsystem.

a) Login to any server in the Mediation subsystem as `root` and run:

```
# bc_diag_bulkconfig.sh --save
```

b) Enter the `root` password once you will be asked.
c) The `bulkconfig` file is automatically generated and distributed to all servers in the subsystem.

7. **Revoke root ssh login**

On each IXP server revoke root ssh login.

a) As `root` run:

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

7.2 Upgrade DTO Package

Whenever you will install or upgrade Mediation server to a new version you need to keep DataWarehouse compatible. You need to upgrade the DTO package there. DataWarehouse is being used as an external xDR Storage.
The DataWarehouse is expected to have installed Oracle database and database instance with created login, password, data table space with name DATA_CDR and index table space with name DATA_IND. Such server must be already installed with DTO schema and package.
Such DataWarehouse need to be already added to 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 Mediation 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 Mediation 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
   ```

7.3 Centralized xDR Builders Upgrade

This procedure describes how to trigger the xDR builder installation on the Mediation subsystem from the CCM. Login in the CCM as TklcSrv user and go to the upgrade utility. It is **recommended to proceed with this step after each Mediation subsystem upgrade**, and not to wait all subsystem are upgraded to install all at the same time.

Note: In order to avoid installation issues login on each Mediation server as cfguser and execute the command:

```
$ iaudit -cvf
```

1. **Associate xDR builders RPM with the Mediation subsystem**

   a) Click on **View Builder RPM Status** link on the left tree. This will display a list of all Mediation subsystems.

   b) Before initiating the builder association, make sure the supported platform of the Builder RPM is in accordance with the platform architecture of the Mediation subsystem you want to associate it with.

   c) Choose one or more Mediation subsystems and click on **Associate RPM Package** icon in the tool bar. This will show a popup containing the list of builder RPMs that are uploaded in NSP.

   d) Select required xDR builders RPM and click on the **Associate** button.

   e) After the successful association the list of the subsystems will be updated.
   The **RPM Name** column will contain the new RPM package name and **Association Status** will be marked as OK.

2. **Apply the configuration to the Mediation subsystem**

   a) Go to the NSP application interface main page.

   b) Click **Centralized Configuration**.

   c) Navigate to the **Mediation** view.

   d) Open **Sites**, open the site, and open **Mediation**.

e) Right-click on the subsystem and click on **Apply changes…** from popup menu.
f) Click **Next** button
g) Click **Apply Changes** button.
h) Wait until changes are applied and check there's no error.
Check there's no error in the result window.

3. Install Builder RPM on Mediation

a) Login to the NSP application interface as the TklcSrv user.
b) Click **Upgrade Utility**.
c) Click on **View Builder RPM** Status from the left tree.
d) This will display all the available Mediation subsystem with their respective RPM **Associate Status** and **Install Status**.
e) Before initiating the builder installation make sure the **Builder RPM** that you want to install on the Mediation subsystem is associated with the Mediation subsystem as indicated by **RPM Name** column and **Association Status** should be OK and **Install Status** should be either - or **Not Started**.
f) Select one or more Mediation subsystem and choose **Install RPM Package** from the tool bar.
g) After the successful installation the **Install status** will change to OK.

4. Session Upgrade

a) Go back to NSP application interface main page.
b) Click **Upgrade Utility**.
c) Click **Upgrade Session** link on left tree, this display all the sessions to be upgraded due to upgrade of associated dictionary.
d) 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**.
e) Once session is upgraded its **Upgrade Status** will become **Upgraded Successfully**.

5. Exceptions

After successful completion of xDR Builder Upgrade procedure:

a) Datafeed should be verified to check if they are using either Deprecated or Removed Field and should be upgraded separately.
b) Protraq based reports should be verified to check if they are using either Deprecated or Removed Field and should be upgraded separately.
c) Static enrichment if any configured should be verified to check if they are using either Deprecated or Removed Field and should be upgraded separately.
d) Update the Mediation license if needed and recreate the Mediation session for the obsolete builders

7.4 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.

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

Appendix A. Knowledge Base Procedures

A.1 How to mount the ISO file via iLO2

1. Store the ISO file to the local disk.
2. Open a web browser and enter the IP address of server iLO. After security exception a login page will appear. Log in as `root`.
3. Navigate to the **Remote Console** tab.
4. Click on **Integrated Remote Console.**
   An **Integrated Remote Console** window appears.
5. Click on **Virtual Media** which is visible in blue bar at the top of the **Integrated Remote Console** window.
6. Navigate to **Image** with a small CD-ROM picture on the left side. Click on **Mount**.
   A window will pop up asking for the ISO path. Navigate to the ISO file and click **Open**.
7. 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 display a virtual CD-ROM media with the exact device name. Example output:
   ```
   # getCDROMmedia
   HP Virtual DVD-ROM:scd0
   ```
   this record denotes virtual CD-ROM device `/dev/scd0` ready for any other operation.

A.2 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**
   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 ⊙ Manage Software Images**
   b) On the next screen choose image, put description and press Add New Image.
   c) Wait till the adding of image is completed.
3. **Record the path of the ISO**
   a) On the command line of the management server running PM&C, run the exportfs command to list the paths of the exported ISOs.
   ```
   # exportfs
   ```
   b) In the sample output below, there are 5 ISOs exported, the PM&C application, TPD, NSP package, Oracle and WebLogic You will need record the path of the ISO that you want to mount on a blade, as this path will be required in the mount command.
   ```
   # exportfs
   /usr/TKLC/smac/html/TPD/PMAC--2.2.0_22.4.0--872-1818-01     169.254.102.0/24
   /usr/TKLC/smac/html/TPD/TPD--3.2.0_62.12.0—TPD              169.254.102.0/24
   /usr/TKLC/smac/html/TPD/NSP--7.0.0_3.5.0--872-2128-101      169.254.102.0/24
   /usr/TKLC/smac/html/TPD/Oracle--10.2.0.3-8--872-2115-01     169.254.102.0/24
   /usr/TKLC/smac/html/TPD/Weblogic--10.3-1.2.0--872-2114-101  169.254.102.0/24
   ```
4. **Login to blade server**

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

5. **Start portmap service**
   As `root` run:
   ```
   # service portmap start
   ```
6. **Start nfslock service**
   As `root` run:
   ```
   # service nfslock start
   ```
7. **Create ISO mount point**
   As `root` run:
   ```
   # mkdir /mnt/local_mount_point
   ```
   where *local_mount_point* is the ISO mount point on the local blade server. Example:
   ```
   # mkdir /mnt/oracle_iso
   ```
8. **Mount ISO**
   As `root` run:
   ```
   # mount management_server_ip:export_path local_mount_point
   ```
   where *management_server_ip* is the control network IP address of the PM&C server, *export_path* is the export path you received in step 3 and *local_mount_point* is the mount point you have created in step 7. Example:
   ```
   # mount 169.254.102.4:/usr/TKLC/smac/html/TPD/oracle_10_1_0_2 /mnt/oracle_iso
   ```

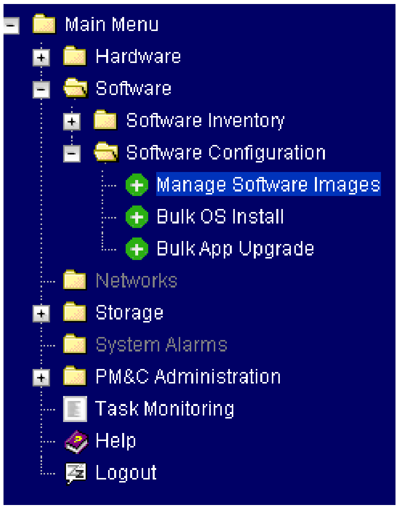
A.3 Adding ISO Images to the PM&C Image Repository

This procedure will provide the steps how add ISO images to PM&C repository.
IF THIS PROCEDURE FAILS, CONTACT ORACLE'S TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

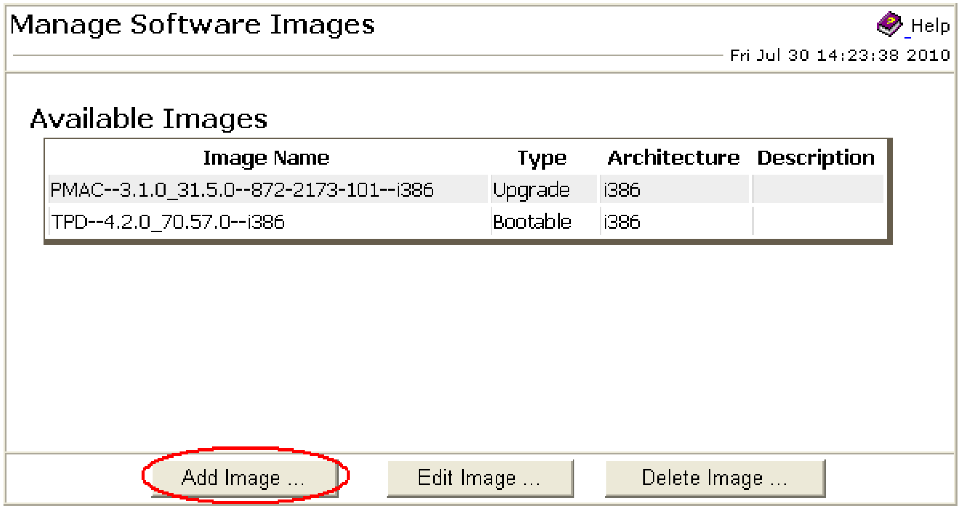
1. Make the image available to PM&C
   There are two ways to make an image available to PM&C:
   a) Insert the CD containing an ISO image into the removable media drive of the PM&C server.
   b) Use sftp to transfer the ISO image to the PM&C server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
      - cd into the directory where your ISO image is located (not on the PM&C server)
      - Using sftp, connect to the PM&C management server
        - ➢ **sftp pmacftpusr@<PM&C_management_network_IP>**
        - ➢ **put <image>.iso**
      - After the image transfer is 100% complete, close the connection
        - ➢ **quit**

2. **PM&C GUI:** Login
   Open web browser and enter:
   http://192.168.1.1/gui
   where 192.168.1.1 is the IP of the Management network.
   Login as pmacadmin user.

3. **PM&C GUI:** Navigate to Manage Software Images
Navigate to Main Menu ⦿ Software ⦿ Software Configuration ⦿ Manage Software Images



4. **PM&C GUI:** Add image
   Press the **Add Image** button.



Manage Software Images

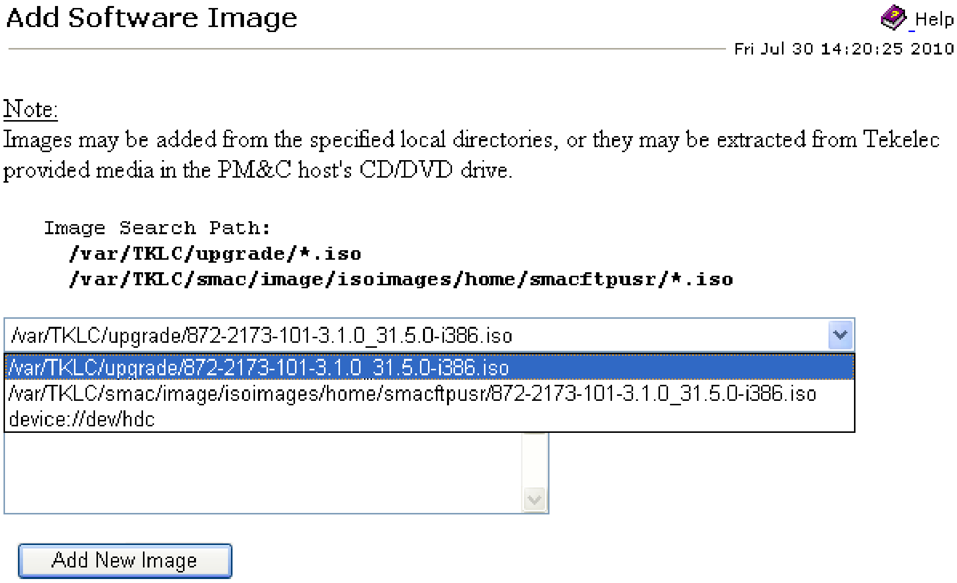
Help

Fri Jul 30 14:23:38 2010

Available Images

Image Name	Type	Architecture	Description
PMAC--3.1.0_31.5.0--872-2173-101--i386	Upgrade	i386	
TPD--4.2.0_70.57.0--i386	Bootable	i386	

Use the dropdown to select the image you want to add to the repository.
Note: Optical media device appears as device **:** `//dev/hdc`
Add appropriate image description and press **Add New Image** button.



Add Software Image

Help

Fri Jul 30 14:20:25 2010

Note:
Images may be added from the specified local directories, or they may be extracted from Tekelec provided media in the PM&C host's CD/DVD drive.

```
Image Search Path:
  /var/TKLC/upgrade/*.iso
  /var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso
```

/var/TKLC/upgrade/872-2173-101-3.1.0_31.5.0-i386.iso

/var/TKLC/upgrade/872-2173-101-3.1.0_31.5.0-i386.iso
/var/TKLC/smac/image/isoimages/home/smacftpusr/872-2173-101-3.1.0_31.5.0-i386.iso
device://dev/hdc

You may check the progress using the `Task Monitoring` link. Observe the green bar indicating success.

A.4 How to connect a server console using iLO ssh connection

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

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

</>hpiLO->
```

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

```
</>hpiLO-> vsp

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

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

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

hostname1368545964 login: root
Password:
```

Appendix B. 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.

Appendix C. 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 Industries, click the link for Oracle Communications documentation.

   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.