Oracle® Communications Performance Intelligence Center

Maintenance Guide

Release 10.1

E53511 Revision 3

January 2015

ORACLE®

Oracle Communications Performance Intelligence Center Maintenance Guide, Release 10.1

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

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

See more information on MOS in the Appendix section.

Contents

1 Introduction

1.1 Documentation Admonishments

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

Table 1: Admonishments

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

1.2 Reference Documents

[1] Platform 6.5 Configuration Procedure Reference 909-2249-001 Revision A, December 2013

[2] TPD Initial Product Manufacture 909-2130-001 Revision D, December 2013

[3] PM&C 5.5 Disaster Recovery 909-2283-001 Rev A, December 2013

[4] EAGLE SW Compatibility Matrix SS005887 v19

[5] PIC Installation document,E53508-01.docx

[6] PIC Upgrade document, E53509-01.docx

[7] Migration Guidelines G5 to Gen8- 10.0 TR007444

[8] Tekelec Platform Initial Product Manufacture Release 5.5 909-2229-001 Revision B

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 procedures to maintenance PIC system at Release 9.0. This document covers disaster recovery procedures, IP change procedures as well as various application specific procedures.

This document is intended for use by internal Tekelec manufacturing, PSE, SWOPS, and many times partners trained in maintenance on both rackmount and c-class blades system. A working-level understanding of Linux and command line interface is expected to successfully use this document.

It is strongly recommended that prior to performing any operations on either a rackmount or c-class blades system, the user read through this document.

Note: The procedures in this document are not necessarily in a sequential order. There are flow diagrams and high-level overview procedures 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 maintenance of the PIC system should reference these flow diagrams and high-level overview procedures during this process

1.5 Requirements and Prerequisites

1.5.1 Hardware Requirements

PIC release 10 doesn't support anymore TEK1/TEK2/Tek3/HP version servers less than G6.

1.5.2 Software Requirements

The following software is required for the PIC 10 installation.

Oracle Communication GBU deliverables:

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

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

https://edelivery.oracle.com/

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

- WebLogic 10.3.5.0 for 64bits JVM support product
    - wls1035_generic.jar

http://www.oracle.com/technetwork/middleware/weblogic/downloads/wls-main-097127.html

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

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

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

- Oracle Database 11.2.0.4 64bits product patchset

- p13390677_112040_Linux-x86-64_1of7.zip
- p13390677_112040_Linux-x86-64_2of7.zip
- p13390677_112040_Linux-x86-64_3of7.zip

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

1.5.3 Licenses Requirements

Licenses required for software installation of PIC 10 are embedded licenses and do not require an explicit license key be applied. The exception to this is the license for Business Objects for the Report Server Platform.

The following license is required for this installation:

- BOE License

Note: Take care to backup IXP license file before to DR if possible. If the hardware server is replaced a new license will be required.

2 NSP Disaster Recovery Procedures

2.1 NSP One-Box

This procedure describes the disaster recovery procedure of the NSP One-Box server. This procedure is a highlevel procedure and some of the complex parts are referenced from different procedures. Note: In order to avoid alarm flooding when NSP will restart, JMX agents can be stopped on all system before executing NSP recovery procedure and restarted after. Pending alarms will be lost.

All systems (IXP, xMF, NSP) retained alarms in their JMX agent during NSP unavailability. When NSP restarts, it would receive numerous alarms. It may slow down restart phase and introduce delay (Proportional to unavailability period), before NSP returns to a normal state.

1. **Reinstall Operating System on the NSP server**

   Estimation: 30 min

   Note: In case of C-Class Blades, there is no need to configure the SAN storage. SAN storage has been configured during the installation and as such this configuration will be preserved during the disaster recovery procedure.

   Install the operating system following right procedure:

   - For RMs HP G6 server follows **Install Operating System on G6 Rackmount Servers**
   - For RMs HP Gen8 server follows **Install Operating System on Gen8 Rackmount Servers**
   - For C-class blade follows **IPM Blade Servers Using PM&C Application**

2. **Resize /var/TKLC/partition**

   Once the OS is installed, type the following commands as root user in order to resize /var/TKLC partition. This step needs to be performed on blade and RMS, before installing applications/thirdparty products:

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

3. **Mount oracle volume**

   Estimation: 10 min

   - For C-class blade setup follows **Remount NSP LUN(C-class blades only)**
   - For Rackmount servers follows **Mount oracle volume (Rackmount only)**

4. **NSP one box fresh install**

   Estimation: 70 min

   Complete installation by following the steps:

1. NSP Pre-Install Configuration
2. Install WebLogic
3. Install Oracle Database
4. Install NSP
5. The nightly backup folder NSP_BACKUP contains the optional_modules_list file.This file should be referred to install optional applications that were present before disaster recovery procedure. Install only those optional modules from post installation procedure that are present in this file.

5. **Check permission for backup directory**

   Execute following commands as root:

```
# cd /opt/oracle/backup
# chmod a+w nsp_bakckup_timestamp
# chown root:root nsp_bakckup_timestamp
```

   Where nsp_bakckup_timestamp refers to the backup directories created nightly

NOTE: NSP creates two different types of backups:

- Backup is generated nightly on oracle server in /opt/oracle/backup/NSP_BACKUP_XX folders. This is the online backup based on an oracle dump to be used during this Disaster recovery procedure.
- An other type of backup is created just before upgrade on oracle server in /opt/oracle/backup/upgrade_backup. This backup is used with backout procedure. This is the offline backup based on database file copy and must not be used During Disaster recovery procedure.

6. **Restore the database and realm**

   Following the steps:

   a. Restore Realm Backup
   b. Recover NSP Database on One-Box setup

7. **Reboot the server**
8. **Install A-Node on Server**

   Following the step Install A-Node on Server
9. **Perform NSP Post-Install Sanity Check**

   Following the step NSP Post-Install Sanity Check (onebox and four box).

2.2 NSP Four-Box

In order to keep the coherence between servers this procedure must be executed completely on all the bowes. It is not possible to use it only on one of the box.

The servers must be backout in the order described bellow:

1. Apache server
2. Oracle server
3. Weblogic Secondary server
4. Weblogic Primary server

Note: During major backout TPD for all the servers can be done in parallel.

2.2.1 Apache Server (Four-Box)

This procedure describes the disaster recovery procedure of the NSP Apache (Four-Box) server. This procedure is a highlevel procedure and some of the complex parts are referenced from different procedures.

Note: In order to avoid alarm flooding when NSP will restart, JMX agents can be stopped on all system before executing NSP recovery procedure and restarted after. Pending alarms will be lost.

All systems (IXP, xMF, NSP) retained alarms in their JMX agent during NSP unavailability. When NSP restarts, it would receive numerous alarms. It may slow down restart phase and introduce delay (proportional to unavailability period) before NSP return to a normal state.

1. **Reinstall Operating System on the NSP server**

   Estimation: 30 min

   Note: In case of C-Class Blades, there is no need to configure the SAN storage. SAN storage has been configured during the installation and as such this configuration will be preserved during the disaster recovery procedure.

   Install the operating system following right procedure:

   - For RMs HP G6 server follows Install Operating System on xMF G6 Rackmount Servers
   - For RMs HP Gen8 server follows Install Operating System on Gen8 Rackmount Servers
   - For C-class blade follows IPM Blade Servers Using PM&C Application

2. **Resize /var/TKLC/partition**

   Once the OS is installed, type the following commands as root user in order to resize /var/TKLC partition. This step needs to be performed on blade and RMS, before installing applications/thirdparty products:

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

3. **Complete the NSP Apache installation**

   Complete installation by following the steps:
   1. NSP Pre-Install Configuration
   2. Install NSP

4. **Reboot the NSP Apache server**
5. **Perform NSP Post-Install Sanity Check**

   Following the step NSP Post-Install Sanity Check (onebox and four box).

2.2.2 Oracle Server (Four-Box)

This procedure describes the disaster recovery procedure of the NSP Oracle server (Four-Box). This procedure is a highlevel procedure and some of the complex parts are referenced from different procedures.

Note: Before executing this procedure external backup must be available. This procedure is also applicable when only MSA is corrupted.

1. **Reinstall Operating System on the NSP server**

   Estimation: 30 min

   Note: In case of C-Class Blades, there is no need to configure the SAN storage. SAN storage has been configured during the installation and as such this configuration will be preserved during the disaster recovery procedure.

   Install the operating system following right procedure:

   - For RMs HP G6 server follows Install Operating System on xMF G6 Rackmount Servers
   - For RMs HP Gen8 server follows Install Operating System on Gen8 Rackmount Servers
   - For C-class blade follows IPM Blade Servers Using PM&C Application

2. **Resize /var/TKLC/partition**

   Once the OS is installed, type the following commands as root user in order to resize /var/TKLC partition. This step needs to be performed on blade and RMS, before installing applications/thirdparty products:

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

3. **Mount oracle volume**

   Estimation: 10 min

   - For C-class blade setup follows Remount NSP LUN(C-class blades only)
   - For Rackmount servers follows Mount oracle volume (Rackmount only)

4. **Install the oracle server**

   Complete installation by following the steps:

   1. NSP Pre-Install Configuration
   2. Install Oracle Database
   3. Install NSP

5. **Check permission for backup directory**

   Execute following commands as root:

   ```
   # cd /opt/oracle/backup
   # chmod a+w nsp_bakckup_timestamp
   # chown root:root nsp_bakckup_timestamp
   ```

   Where nsp_bakckup_timestamp refers to the backup directories created nightly

NOTE: NSP creates two different types of backups:

- Backup is generated nightly on oracle server in /opt/oracle/backup/NSP_BACKUP_XX

folders. This is the online backup based on an oracle dump to be used during this Disaster recovery procedure.

- An other type of backup is created just before upgrade on oracle server in /opt/oracle/backup/upgrade_backup. This backup is used with backout procedure. This is the offline backup based on database file copy and must not be used During Disaster recovery procedure.

6. **Restore the oracle database**

   Following the steps: Recover NSP Database on Four-Box setup

7. **Reboot the NSP Oracle server**
8. **Perform NSP Post-Install Sanity Check**

   Following the step NSP Post-Install Sanity Check (onebox and four box).

2.2.3 Secondary WebLogic (Four-Box)

This procedure describes the disaster recovery procedure of the NSP Secondary WebLogic (Four-Box) server. This procedure is a highlevel procedure and some of the complex parts are referenced from different procedures.

1. **Reinstall Operating System on the NSP server**

   Estimation: 30 min

   Note: In case of C-Class Blades, there is no need to configure the SAN storage. SAN storage has been configured during the installation and as such this configuration will be preserved during the disaster recovery procedure.

   Install the operating system following right procedure:

   - For RMs HP G6 server follows Install Operating System on xMF G6 Rackmount Servers
   - For RMs HP Gen8 server follows Install Operating System on Gen8 Rackmount Servers
   - For C-class blade follows IPM Blade Servers Using PM&C Application

2. **Resize /var/TKLC/partition**

   Once the OS is installed, type the following commands as root user in order to resize /var/TKLC partition. This step needs to be performed on blade and RMS, before installing applications/thirdparty products:

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

3. **Complete the NSP Secondary WebLogic Installation**

   Complete installation by following the steps:

   4. NSP Pre-Install Configuration
   5. Install WebLogic
   6. Install NSP

4. **Recover the Primary server**

   Following the steps: Primary WebLogic (Four-Box)

5. **Reboot the NSP Secondary server**
6. **Perform NSP Post-Install Sanity Check**

   Following the step NSP Post-Install Sanity Check (onebox and four box).

2.2.4 Primary WebLogic (Four-Box)

This procedure describes the disaster recovery procedure of the NSP Primary WebLogic server (Four-Box). This procedure is a highlevel procedure and some of the complex parts are referenced from a different procedures.

1. **Reinstall Operating System on the NSP server**

   Estimation: 30 min

   Note: In case of C-Class Blades, there is no need to configure the SAN storage. SAN storage has been configured during the installation and as such this configuration will be preserved during the disaster recovery procedure.

   Install the operating system following right procedure:

   - For RMs HP G6 server follows Install Operating System on xMF G6 Rackmount Servers
   - For RMs HP Gen8 server follows Install Operating System on Gen8 Rackmount Servers
   - For C-class blade follows IPM Blade Servers Using PM&C Application

2. **Resize /var/TKLC/partition**

   Once the OS is installed, type the following commands as root user in order to resize /var/TKLC partition. This step needs to be performed on blade and RMS, before installing applications/thirdparty products:

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

3. **Prepare server for recovery**

   IMPORTANT: This step is crucial and MUST NOT be omitted! Omitting this step **WILL** result in data loss

   Open a terminal window and log in to NSP Primary WebLogic server as root

   ```
   # touch /opt/recovery
   ```

4. **Restore optional modules files**

   Copy the optional modules list file from backup into /tmp
   As root run:

```
# scp
oracle_ip_address:/opt/oracle/backup/nsp_backup_dir/primary/optional_modules
_list /tmp
```

Where oracle_ip_address is the IP address of NSP Oracle server and nsp_backup_dir is the nightly backup directory and the optional modules list can be found in its primary subdirectory

5. **Complete the NSP Primary WebLogic Installation**

   Complete installation by following the steps:
   1. NSP Pre-Install Configuration
   2. Install WebLogic
   3. Install NSP

6. **Import the Realm**

   Following the steps:Restore Realm Backup

7. **Reboot all the NSP cluster**

   Reboot all 4 NSP servers from the Four-Box setup:
   1. Apache server
   2. Oracle server
   3. Weblogic Secondary server
   4. Weblogic Primary server

8. **Install A-Node on Server**

   Following the steps Install A-Node on Server

9. **Restore SNMP and SMTP configuration**
   a. For SNMP, follow the Modify SNMP Agent IP Address procedure in **PIC Installation document**
   b. For SMTP, follow the Configure Mail Server procedure in in **PIC Installation document**
10. **Perform NSP Post-Install Sanity Check**

    Following the step NSP Post-Install Sanity Check (onebox and four box).

2.3 Mount oracle volume (Rackmount only)

Run this procedure as root:

1. **Mount NSP ISO**

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

Where *iso_path* is the absolute path of the ISO image including name of the image (for example, /var/TKLC/upgrade/iso_file_name.iso).

2. **Mount oracle volume**

```
# sh /mnt/upgrade/scripts/mount_oracle_part.sh
```

3. **Umount ISO**

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

2.4 Remount NSP LUN(C-class blades only)

This procedure describes the steps to remount the logical volumes from MSA2012fc to NSP server.

Prerequisite:

- The NSP one box server or oracle server of a four boxes config must be IPM, with network and other system parameters set, the same way as for a fresh install.
- Password of platcfg user must be already known.

1. **Login as root user on the NSP server for onebox setup or oracle server of a four box NSP (all following commands are executed as root)**
2. **Retrieve LUN numbers of logical volumes**

```
# multipath –ll
```

The result will display 2 blocks of lines starting with **mapth0** and **mapth1** as in following example:

```
mpath0 (3600c0ff000d5809fb180cc4901000000) dm-6 HP,MSA2012fc
[size=70G][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:0:37 sdc 8:32  [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 1:0:0:37 sdd 8:48  [active][ready]
mpath1 (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc
[size=419G][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:1:36 sda 8:0   [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 1:0:1:36 sdb 8:16  [active][ready]
mpath2 (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc
[size=139G][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:1:35 sde 8:64   [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 1:0:1:35 sdf 8:80  [active][ready]
```

The lun# is the 4th number in the 4th and 6th line of each block, here in the example:

- Lun# for REDO is the one in the block containing [size=70G] (37 for mpath0 in example)
- Lun# for DATA is the one in the block containing [size=419G](36 for mpath1 in example)
- Lun# for BACKUP is the one in the block containing [size=139G](35 mapth2 in example)

3. **Recreate mapping to SAN REDO volume**

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

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

b. When prompted for **Login on Remote** with the user `platcfg`

c. After completion, the output must show:

```
<result>
1
</result>
```

4. **Recreate mapping to SAN DATA volume**

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

```
# tpdProvd --client --subsystem=TPD::SOAP::Storage addVolumeInfo lun
36 name nsp_data_vol mount /opt/oracle/oradata
```

b. When prompted for **Login on Remote** with the user `platcfg`

c. After completion, the output must show:

```
<result>
1
</result>
```

5. Recreate mapping to SAN BACKUP volume

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

```
# tpdProvd --client --subsystem=TPD::SOAP::Storage addVolumeInfo lun
35 name nsp_backup_vol mount /opt/oracle/backup
```

b. When prompted for **Login on Remote** with the user `platcfg`

c. After completion, the output must show:

```
<result>
1
</result>
```

6. Check the volume names

```
# multipath -ll
```

It will display 3 blocks of lines starting with **mapth0**, **mapth1** and **mpath2** as in following example:

```
nsp_redo_vol (3600c0ff000d5809fb180cc4901000000) dm-6 HP,MSA2012fc
[size=70G][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:0:37 sdc 8:32  [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 1:0:0:37 sdd 8:48  [active][ready]

nsp_data_vol (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc
[size=419G][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:1:36 sda 8:0   [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 1:0:1:36 sdb 8:16  [active][ready]

nsp_backup_vol (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc
[size=139G][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:1:35 sde 8:64   [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 1:0:1:35 sdf 8:80  [active][ready]
```

It should no longer show **mapth0**, **mpath1** and **mpath2**.

7. Check the file system

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

8. **Mount the volumes**

```
# mount -a
```

9. **Verify the volumes**

```
# df -h


Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root
                     496M  123M  349M  26% /
/dev/cciss/c0d0p1    122M  9.9M  106M   9% /boot

none                 4.0G     0  4.0G   0% /dev/shm
/dev/mapper/vgroot-plat_tmp
                    1008M   47M  910M   5% /tmp
/dev/mapper/vgroot-plat_usr
                     4.0G  1.1G  2.7G  30% /usr
/dev/mapper/vgroot-plat_var
                     496M   40M  431M   9% /var
/dev/mapper/vgroot-plat_var_tklc
                     4.0G   68M  3.7G   2% /var/TKLC
/dev/mapper/nsp_redo_vol
                    69G  4.2G   61G   7% /usr/TKLC/oracle/ctrl1
/dev/mapper/nsp_data_vol
```

2.5 NSP Pre-Install Configuration

This procedure describes how to configure the NSP servers, which is required prior to install the NSP application.

This procedure consists of several actions that are needed to configure the NSP servers:

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

- Configure the NSP server hostname.
  Note: This configuration is required to get the hardware alarms forwarded by the system as SNMP traps into NSP ProAlarm.

- Configure SNMP.
- Add cdrom entry to /etc/fstab.
  Note: The purpose of adding this entry is to simplify mount commands that will be used throughout the NSP installation process.

Before you perform this procedure, make sure you have read and are familiar with the PIC Bulkconfig File Description
This procedure must be performed on each NSP server (single server for a one-box; all four servers for a four-box).

1. **Login as root user on the NSP server for onebox setup or oracle server of a four box NSP (all following commands are executed as root)**
2. **Check system healt**

```
# syscheck
```

If any error is detected find the detail of the erro in `/var/TKLC/log/syscheck/fail_log`

Example ouput for a healthy system:

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

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

3. **Create the bulkconfig file (or copy the file from an other server)**
4. **Configure the server hostname**

a. Enter the **platcfg**

```
# su - platcfg
```

b. Select **Server Configuration ⊙ Hostname**
c. Click **Edit**
d. Type the NSP server hostname and click **OK**
e. Return to the main **platcfg** menu

5. **Configure SNMP**

a. From the main platcfg menu, select Network Configuration➢SNMP Configuration➢NMS
b. Configuration and select Edit > Add A New NMS Server.
c. Enter
Hostname or IP: 127.0.0.1
Port: 162
SNMP Community String: TEKELEC
and then click OK and then EXIT
d. Click YES to restart alarm server and then press any Key to continue.
e. Exit the platcfg menu.

2.6 Install WebLogic

This procedure describes how to install the WebLogic software for the NSP (single server for a One-

box; On the designated Primary and Secondary WebLogic servers for a Four-box). Before you perform this procedure:

- Make sure that you have the WebLogic files available.
- Verify the /root/bulkconfig file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.

Note: Run this procedure via ILO.

2.6.1 Mount NSP media

As root, run:

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

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

2.6.2 Install WebLogic Product

As root, run:

```
# /mnt/upgrade/install_weblogic.sh
```

Wait until the installation process is complete.

Analyze the installation log

Verify that WebLogic installed successfully.

In the WebLogic Software Installation log (/var/TKLC/log/upgrade/weblogic.log), the

"Weblogic product is installed successfully" message appears at the end of the file.

If this message does not appear in the log file, contact the Oracle Customer Care Center.

2.7 Install Oracle Database

This procedure describes how to install the Oracle database on a server with the operating system installed (TPD).

Before you perform this procedure:

- Make sure that you have the Oracle files available.
- Verify the /root/bulkconfig file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.
- In case of c-class blades SAN Configuration must be done properly before starting Oracle Installation

Note: Run this procedure via ILO.

As root, run:

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

Wait until the installation process is complete.

Note: the system will reboot at the end of Oracle database product installation

Analyze the installation log:

Verify that Oracle installed successfully.

In the Oracle product Installation log (/var/TKLC/log/upgrade/oracle.log), the

Oracle product is installed successfully message appears at the end of the file.

If this message does not appear in the log file, contact the Oracle Customer Care Center.

2.8 Install NSP

2.8.1 Mount NSP media

As root, run:

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

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

2.8.2 Install NSP application

As root, run:

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

Wait until the installation process is complete.

Analyze the installation log:

Verify that NSP installed successfully.

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 2.12` NSP Post-Install Sanity Check (onebox and four box)

2.9 Restore Realm Backup

This procedure describes how to restore the NSP realm backup.
NOTE: During Disaster recovery the Nightly Backup present at /opt/oracle/backup/ folder with names NSP_BACKUP_dd_mm_yy_hh_mm_ss must be used

1. Log in as `root` on NSP (One-box) or NSP Primary WebLogic (Four-Box) – all following commands are executed as root
2. Copy the realm backup into a local directory:

   ```
   # scp –r oracle_ip_address:/opt/oracle/backup/nsp_backup_dir/ /usr/TKLC/nsp/
   ```

   Where oracle_ip_address is the IP address of NSP Oracle server and nsp_backup_dir is the nightly backup directory and the optional modules list can be found in its primary subdirectory.

3. Execute the following commands:

   Note: Make sure the backup is from the same NSP release which needs to be imported
   Note: Make sure the backup directory is owned by tekelec user. If not change ownership to tekelec before running command below

   ```
   # cd /opt/nsp/scripts
   # ./LaunchImpNSPrealm.sh backup_dir
   ```

Where backup_dir is the direcory which contains the backup of realm data (e.g. /usr/TKLC/nsp/NSP_BACKUP_10_14_10_22_00_01/)

2.10 Recover Database

2.10.1 Recover NSP Database on One-Box setup

This section describes the various steps and methods for using import utility to restore NSP database.

1. **Prerequisites for using Import Utility to Restore a Database**

   The import procedure reloads a previous export file, partially or completely, back into an NSP database. All following scripts must be run as OS user root.

   Restoring the database can occur for a variety of reasons and it is not possible to provide automatic restoration procedures for every case.

   - Prerequisite for restoring a database

     NSP data backup is required as a prerequisite for restore process. During the oracle restore operation the weblogic service must be stop to avoid any user connection

     Note: Ensure that the directory containing database dump to restore has write permissions for oracle user.

     Otherwise use the following command to set write permission:

     ```
     # chmod a+r+w+x <DIR_CONTAINING_DUMP>
     ```

     Note: Check the ownership of ExpNSP.dmp.gz inside the <DIR_CONTAINING_DUMP>. If the ownership is not oracle:oinstall, perform the below step

     As root user go to folder <DIR_CONTAINING_DUMP>:

     ```
     # chown oracle:oinstall ExpNSP.dmp.gz
     ```

   - Common reasons for restoring a database
     - Disk failure
     - Hardware extension
     - Accidental deletion of data by operator
     - Migration
     - Transfer on another server
     - Reprocessing of archives

2. **Import utility**

   The results provided by the backup are standard dump files produced by Oracle. They must be put online again to be able to import them. Importing of saved data occurs with the import utility provided by Oracle.The scripts are provided with an NSP database installation

   The Import scripts are located in the installation directory of the NSP database `opt/nsp/scripts/oracle.`

This directory contains the three same subdirectories listed in **Export scripts**:

- cmd - contains OS shell scripts
- sql - contains SQL procedures called by the shell scripts
- trc - contains traces or output files location

a. Log in as `root` on NSP (One-box) and launch the command:

```
# service nspservice stop
```

b. Login as `root` user on NSP Server for one-box and launch the command:

```
# cd  /opt/nsp/scripts/oracle/cmd
# ./RestoreDatabase.sh NSP/NSP NSP NSP <backup_dir>
```

The command restores the NSP database after stopping the Oracle listener. After the restore is complete the Oracle listener is restarted.

The script has four parameters:

- Oracle connection string (NSP/NSP) must not be modified
- Name of the exported schema name (NSP) must not be modified
- Target schema name (NSP) must not be modified
- The `backup_dir` is the path of the directory which contains the exported database file (**ExpNSP.dmp**).

c. Check the generated log files in `/opt/nsp/scripts/oracle/trc` directory for possible errors.

d. Log in as `root` on NSP (One-box) and launch the command:

```
# service nspservice start
```

2.10.2 Recover NSP Database on Four-Box setup

This section describes the various steps and methods for disaster recovery of NSP database.

1. **Prerequisites for using Import Utility to Restore a Database**

   The import procedure reloads a previous export file, partially or completely, back into an NSP database. All following scripts must be run as OS user root.

   Note: In Four-Box clusters the script must be executed on NSP Oracle box.

   Restoring the database can occur for a variety of reasons and it is not possible to provide automatic restoration procedures for every case.

   - Prerequisite for restoring a database

     NSP data backup is required as a prerequisite for restore process. During the oracle restore operation the weblogic service must be stop to avoid any user connection

     Note: Ensure on Oracle Box that the directory containing database dump to restore has write permissions for oracle user.

     Otherwise use the following command to set write permission:

a. Login as root on NSP Oracle (Four-Box).

```
# chmod a+r+w+x <BACKUP_DIR>
# chmod a+r+w+x <DIR_CONTAINING_DUMP>
```

Ex: <BACKUP_DIR> = NSP_BACKUP_06_12_12_22_00_01/
<DIR_CONTAINING_DUMP> = NSP_BACKUP_06_12_12_22_00_01/oracle

Note: Check the ownership of ExpNSP.dmp.gz inside the <DIR_CONTAINING_DUMP>. If the ownership is not oracle:oinstall, perform the below step

As root user go to folder <DIR_CONTAINING_DUMP>:

```
# chown oracle:oinstall ExpNSP.dmp.gz
```

- Common reasons for restoring a database
  - Disk failure
  - Hardware extension
  - Accidental deletion of data by operator
  - Migration
  - Transfer on another server
  - Reprocessing of archives

2. Stop WebLogic

a. Login as root on NSP Primary WebLogic (Four-Box). As root run:

```
# service nspservice stop
```

3. Restore the NSP database

Note: In case MSA was also faulty and replaced , make sure external backup of (ExpNSP.dmp.gz is copied to <backup_dir> and has oracle ownership.

a. Login as root on NSP Oracle (Four-Box).

b. The following command restores the NSP database after stopping the Oracle listener. After the restore is complete the Oracle listener is restarted. As root run:

```
# cd /opt/nsp/scripts/oracle/cmd
# ./DisasterRecoveryDatabase.sh NSP/NSP NSP NSP backup_dir
```

The script has four parameters

- Oracle connection string (NSP/NSP) must not be modified
- Name of the exported schema name (NSP) must not be modified
- Target schema name (NSP) must not be modified
- The backup_dir is the path of the directory which contains the exported database file(**ExpNSP.dmp.gz**).

Ex: backup dir = /opt/ oracle/backup/NSP_BACKUP_06_12_12_22_00_01/oracle

c. Check the generated log files in /opt/nsp/scripts/oracle/trc directory for possible errors.

4. Restart weblogic

a. Login as root on NSP Primary WebLogic (Four-Box). As root run:

```
# service nspservice start
```

2.11 Install A-Node on Server

1. Open a terminal window and log in on NSP Primary Web-Logic serveras root
2. Insert the xMF CD to the cdrom
3. If ISO is available copy the iso to NSP primary server at some location
4. Install the A-Node. As root run:

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

When asked for ISO, provide the complete ISO path (e.g. /var/TKLC/upgrade/isoname.iso)

5. Type yes to confirm
6. No reboot need

NOTE (WORKAROUND PR 216438):- During Onebox Server Disaster recovery user needs to apply following workaround in order to deploy missing application

Login as tekelec user on NSP Server

```
$ cd /opt/nsp/nsp-package/bundle-ws
$ ant app.deploy
$ cd /opt/nsp/nsp-package/dicohelp
$ ant app.deploy
```

Switch to root user and run:

```
# service nspservice restart
```

2.12 NSP Post-Install Sanity Check (onebox and four box)

Box: Onebox /Four Box

1. Open a terminal window and log in as root on the NSP One-box or each box of Four-box system.
2. As root, run:

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

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

3. Review the NSP installation logs (/var/log/nsp/install/nsp_install.log).
4. 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
```

3 xMF Disaster Recovery Procedures

3.1 xMF Server Disaster Recovery

1. **Reinstall Operating System**
    - For RMs HP G6 server follows Install Operating System on G6 Rackmount Servers
    - For RMs HP Gen8 server follows Install Operating System on Gen8 Rackmount Servers
    - For E5-APP-B server follow Install Operating System on E5-APP-B Servers

2. **Refer to Installation document, chapter 5 XMF APPLICATION INSTALLATION PROCEDURES till section 5.3 Install xMF.**
3. **Refer to Upgrade Document, section 6.4 Sync NSP with xMF and 6.5 xMF Post-Sync Healthcheck**

Note: In case of IMF sub-system and if disaster recovery procedure has been run on all servers of a sub-system, then the “Apply change” procedure on NSP will fail because sub-system VIP has been lost. In this case step 3 mentioned above should be executed.

4 IXP/DWS Disaster Recovery Procedures

4.1 IXP/DWS Disaster Recovery Overview

This section describes how to execute a disaster recovery procedure on the IXP server.

The procedure is applicable to the following server types:

- DWS Server
- IXP PDU Storage Server
- IXP Base Server

The procedure is applicable to the following hardware types:

- HP G6 RackMount
- HP G6 C-Class Blade
- HP Gen8 RackMount
- HP Gen8 C-Class Blade

Note on DWS: During the disaster recovery procedure of DWS Server you must install the same version of the Oracle database as the current one. However, this procedure only applies to DWS freshly installed as part of PIC 10. Thus, if Oracle 10g is installed, the disaster recovery procedure can not be applied and you have to go for a new installation (refer to the installation document [5] , section INSTALLATION OVERVIEW FOR DWS).
If Oracle 11g is currently installed then the disaster recovery procedure for DWS can be executed. Check the Oracle version on the DWS Server as root with the following command:

```
# rpm -q tklc-oracle-dbms
```

Note on IXP: It is recommended to redistribute DFPs assigned to the recovering server to other IXP server in the IXP subsystem. Any DFPs assigned to recovering server will not be functional during disaster recovery. Refer to Offload DFPs from the IXP Server

4.1.1 DWS server disaster recovery procedure

Follow the references below in a sequential order to recover the DWS server.

1. **Set the DWS in** MAINTENANCE mode
2. Retrieve LUN numbers of logical volumes **(C-class blades only)**
3. **Refer to Installation document [5] , section INSTALLATION OVERVIEW FOR DWS**
   Note: bulkconfig file must contain DR-XDR plateform function value.
   Note: **for C-class blades setup**, don't run SAN configuration step but run Remount LUN.
4. **If the DWS was active before the DR, reset it in** ACTIVE mode.

4.1.2 IXP PDU Storage server disaster recovery procedure.

Follow the references below in a sequential order to recover the IXP PDU Storage server:

1. Stop IXP Service
2. Disintegrate Server with the IXP Subsystem
3. Retrieve LUN numbers of logical volumes **(C-class blades only)**
4. **Refer to Installation document [5] , section INSTALLATION OVERVIEW FOR IXP**
   Note: bulkconfig file must contain DR-PDU plateform function value.
   Note: **for C-class blades setup**, don't run SAN configuration step but run Remount LUN.
5. **Accept the upgrade:**
   a. **As** `root`**, enter in platcfg menu:**
      ```
      # su - platcfg
      ```
   b. **Enter in Maintenance / Upgrade menu**

c. **Select Accept upgrade**

6. Integrate Server with the IXP Subsystem
7. Remount Export Directories

4.1.3 IXP Base server disaster recovery procedure.

Follow the references below in a sequential order to recover IXP Base server: IXP PDU Storage server disaster recovery procedure.

Note: bulkconfig file must contain DR-BASE plateform function value.

4.2 Stop IXP Service

This procedure describes how to stop the IXP service on the IXP server.

Open a terminal as root on the IXP server:

```
# service TKLCixp stop
```

4.3 Disintegrate Server with the IXP Subsystem

This procedure describes how to disintegrate an IXP server with the IXP subsystem.

1. **Analyze subsystem**
   - **a)** Open a terminal window and log in to any IXP server in the IXP subsystem, except the server you want to disintegrate.
   - **b)** Check that the subsystem is in good shape. As `cfguser`, run:

     ```
     $ analyze_subsystem.sh
     ```

     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 (ignore error messages regarding the server that is going to be disintegrated for the subsystem).
     If errors occur, contact the Tekelec Customer Care Center.

2. **Remove a host record from the bulkconfig file**
   - **a)** As `root` user, remove a host record with the server you want to disintegrate from the `/root/bulkconfig` file.
   - **b)** Make sure now the `/root/bulkconfig` file contains all remaining servers in the subsystem with valid parameters.

3. **Update IXP subsystem servers**
   - **a)** Run the following script to adjust the IXP subsystem network and other settings accordingly to the `/root/bulkconfig` file. As `root` run:

     ```
     # bc_adjust_subsystem.sh
     ```

   - **b)** Wait until system reconfigures.
   - **c)** Verify that the IXP subsystem has been reconfigured correctly. As `root` run:

     ```
     # bc_diag_bulkconfig.sh -a
     ```

   - **d)** If any error occurs contact the Tekelec Customer Care Center.

4.4 Integrate Server with the IXP Subsystem

This procedure describes how to integrate recovered server with the IXP subsystem.

1. **Add a host record to the bulkconfig file with the recovered server**
   - **a)** Open a terminal window and log in to the recovered server as `root` user.
   - **b)** Recreate the `/root/bulkconfig` file. You can copy the content of the

`/root/bulkconfig` from any other server in the IXP subsystem.

c) Add a host record for the recovered server with the valid information into the `/root/bulkconfig` file.

d) Make sure now the `/root/bulkconfig` file contains all servers in the subsystem with valid parameters.

2. **Restore shared directories and Data Feed status**

   a) Restore possible shared directories by running, as `root`:

   ```
   # ixp_postinsall_restore.sh
   ```

   b) Restore Data Feed status by running, as `root`:

   ```
   # RestoreDataFeedStatus.sh --local
   ```

3. **Update IXP subsystem**

   Refer to **Update IXP subsystem servers**.

4. **Copy the xDR Builder rpm if not present**

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

   ```
   $ ls /var/TKLC/jmxagent/upload/
   ```

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

   b) Copy the xDR builder rpm to path `/var/TKLC/jmxagent/upload/`

   Note: xDR builder rpm which is mentioned in load line up

5. **Install the xDR Builder package**

   All servers in the IXP subsystem must have the same xDR builders package.

   As `cfguser` run:

   ```
   $ server_builder_installer.sh -f xdr_builder_rpm_filename
   ```

   Where *xdr_builder_rpm_filename* is the name of the builder `*.rpm` package already uploaded in the NSP and associated to this subsystem.

4.5 Remount Export Directories

This procedure describes how to remount export directories for DataFeed application purpose. This procedure is applicable to any DataFeed application hosts (IXP servers). Run this procedure on each DataFeed host that uses his particular Export File Server as an export feed target.

1. **Open a terminal window and log in on the DataFeed application host server as cfguser.**
2. **Unmount the directories. As `cfguser` run:**

   ```
   $ sudo umount /opt/TKLCdataexport/mount/*
   ```

3. **DataFeed will mount exporting directories back by itself.**

4.6 Retrieve LUN numbers (C-class blades only)

This procedure describes how to remount the IXP/DWS LUN. The procedure is applicable to DWS and PDU Storage Server only.

Retrieve volume names and LUN numbers from SAN configuration file

Retrieve all volume names and LUN numbers from the SAN template that has been used to configure the server.

4.7 Remount LUN (C-class blades only)

This procedure describes how to remount the IXP/DWS LUN. The procedure is applicable to DWS

and PDU Storage Server only.

1. **Check the volume are visible from the server.**

   As `root` run:
   ```
   # multipath -ll
   ```
   If the command is returning a result you can proceed with the next step; if not try to reboot the server.

2. **Remount LUN on DWS**

   Note: ignore this step for IXP PDU servers

   a) Repeat the following command for each LUN you need to mount. As `root` run:
   ```
   # /usr/TKLC/plat/bin/tpdProvd --client --subsystem=TPD::SOAP::Storage
   addVolumeInfo name volume_name lun lun_number fstype raw
   ```

   where *volume_name* is the name of the volume you have retrieved from SAN template and *lun_number* is corresponding LUN number you have retrieved from SAN template.

   b) After completion you have to see along with the other output:
   ```
   <result>
   1
   </result>
   ```

3. **Remount LUN on IXP PDU servers**

   Note: ignore this step for DWS

   a) Repeat the following command for each LUN you need to mount. As `root` run:
   ```
   # /usr/TKLC/plat/bin/tpdProvd --client --subsystem=TPD::SOAP::Storage
   addVolumeInfo name volume_name lun lun_number mount mount_dir
   ```

   where *volume_name* is the name of the volume you have retrieved from SAN template, *lun_number* is corresponding LUN number you have retrieved from SAN template and *mount_dir* depends on what server is being updated:
   - `/pdu_1`, when remounting the first PDU filesystem LUN of an IXP PDU server
   - `/pdu_2`, when remounting the second PDU filesystem LUN of an IXP PDU server

   b) After completion you have to see along with the other output:
   ```
   <result>
   1
   </result>
   ```

4. **Check the volume names**

   a) As `root` run:
   ```
   # multipath -ll
   ```

   b) Example output for xDR Storage Server with file based Oracle 10g. Note that `mpath*` entries are renamed and also mounted and such visible in output of the mount command.
   ```
   1_oracle_data (3600c0ff000d5809fb180cc4901000000) dm-6 HP,MSA2012fc
   [size=1.4T][features=0][hwhandler=0]
   \_ round-robin 0 [prio=1][active]
   \_ 0:0:0:37 sdc 8:32  [active][ready]
   \_ round-robin 0 [prio=1][enabled]
   \_ 1:0:0:37 sdd 8:48  [active][ready]
   1_oracle_index (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc
   [size=1.4T][features=0][hwhandler=0]
   \_ round-robin 0 [prio=1][active]
   \_ 0:0:1:36 sda 8:0   [active][ready]
   \_ round-robin 0 [prio=1][enabled]
   \_ 1:0:1:36 sdb 8:16  [active][ready]
   ```

5 PIC IP Changes Procedure

5.1 PIC IP Change Overview

This section describes the IP change procedure for PIC system. This IP change procedure is applicable to already configured PIC system that is in running state.

The procedure below depicts an overall PIC IP change procedure. If some of the components are not meant to be migrated to new network settings skip this step. Otherwise you must follow the sequence.

Note: This procedure must be run via ILO

1. **Disable all feeds associated with IXP subsystems and Export File Server**
   Note: Execute this step if you are going to migrate IXP subsystem or Export File Server.
   a. Open a web browser and log in to NSP application interface and navigate to **DataFeed** application.
   b. Click on **xDR/KPI Feeds** and deactivate all feeds that are associated with the Export Servers or IXP subsystems that going to be migrated to new network settings

2. **NSP IP Change Procedure**
3. **XMF subsystem IP Change Procedure**
4. **IXP Subsystem IP Change Procedure**
5. **DWS IP Change Procedure**
6. **Enable all feeds associated with IXP subsystems and Standalone Export Servers**
   Note: Execute for all feeds that has been disactivated before PIC IP change procedure.
   a. Open a web browser and log in to NSP application interface and navigate to **DataFeed** application.
   b. Click on **xDR/KPI Feeds**
   c. Check feed associated with the affected Export Server(s)
   d. Click on **Modify** icon and navigate to IP address of Export Server. e) Change the IP address and save changes. **Activate** the feed.
   e. Repeate steps c-e for all affected feeds.

5.2 NSP IP Change Procedure

This procedure describes the NSP IP change procedure.
Note: This procedure must be run via ILO

1. **Modify NSP IP Address:**
   - NSP One-Box:
     a. **Modify NSP One-Box IP Address**
   - NSP Four-Boxes:
     a. **Modify NSP Apache IP Address (Four-Box Configuration)**
     b. **Modify NSP Secondary or Oracle IP Address (Four-Box Configuration)**
     c. **Modify NSP Primary IP Address (Four-Box Configuration)**

2. **Update NSP IP addresses on xMF**
3. **Update NSP IP addresses on IXP or EFS**

5.2.1 Modify NSP One-Box IP Address

This procedure describes how to update the IP address on the NSP One-box server.

Run this procedure as root:

1. Open a terminal window and log in as `root` on the NSP One-Box server.
2. Modify NSP server IP address

```
# netAdm set --address={new_onebox_ip} --device={interface} --
netmask={net_mask}
```

Where {new_onebox_ip} is the new IP address of NSP server, e.g.:

- eth01 for Rackmount
- bond0.3 for blade

Where {ipaddress} is the IP address needs to be removed, e.g.172.22.49.10

Where {net_mask} is the mask of network, e.g. 255.255.254.0

If the second interface gateway IP address needs to be modified, repeat this step for the second interface (either eth02 for Rackmount or bond0.4 for blade).

3. Enter the platcfg menu. As root, run:

```
# su - platcfg
```

From the main platcfg menu, select NSP Configuration ➢IP Configuration.

Click Edit.

Click Yes.

The IP address is changed.

Exit the platcfg menu

4. After the IP address is changed , run the command:

```
# su - cfguser -c "setCCMnode new_onebox_ip"
```

Where {new_onebox_ip} is the new IP address of NSP server

5.2.2 Modify NSP Apache IP Address (Four-Box Configuration)

This procedure describes how to update the IP address on the NSP Apache server.

Run this procedure as root:

1. Open a terminal window and log in as `root` on the NSP Apache server.
2. **Follow Steps 1 to 3**Modify NSP One Box IP address

5.2.3 Modify NSP Secondary or Oracle IP Address (Four-Box Configuration)

This procedure describes how to update the IP address on the NSP Secondary or the Oracle server.

Run this procedure as root:

1. Open a terminal window and log in as `root` on the NSP Apache server.
2. **Follow Steps 1 to 3**Modify NSP One Box IP address

5.2.4 Modify NSP Primary IP Address (Four-Box Configuration)

This procedure describes how to update the IP address on the NSP Primary server.

Following the step Modify NSP One-Box IP Address

5.2.5 Update NSP IP addresses on xMF

This procedure describes the steps to update the NSP IP addresses on xMF subsystems.

Run this procedure as root:

1. Update appservers in`/root/bulkconfig` file with appropriate values
2. Following the step XMF subsystem IP Change Procedure

5.2.6 Update NSP IP addresses on IXP or EFS

This procedure describes how to update the NSP IP addresses on the IXP subsystem or EFS servers. This procedure assumes you are familiar with the IXP /root/bulkconfig file.

Note: This procedure is applicable to IXP subsystem and EFS server. Althought this is the same for both applications, the procedure must be executed on IXP subsystem or EFS server separately.

Run this procedure as root:

1. Update the `/root/bulkconfig` file with the new NSP IP addresses
2. Execute following commands:

```
# bc_adjust_subsystem.sh
```

The IP addresses of NSP servers will be changed on all servers in the IXP subsystem or EFS.

5.3 XMF subsystem IP Change Procedure

Use this procedure to change IP addresses of an XMF Subsystem.

Note: This procedure must be run via ILO

5.3.1 Change IP Addresses

Run this procedure as root:

1. Update the `/root/bulkconfig` file with new IP addresses
2. Run bulkconfig script:

```
# /opt/TKLCmf/bin/bulkConf.pl
```

3. Reboot the server

5.3.2 Change VIP Addresses

Note: This is run on the primary server only

1. Login to **primary** server as **cfguser**
2. Run setSSVIP script:
   - If the xMF server is standalone PMF server then execute following command:
     `setSSVIP -s`
   - If the xMF server is primary server of xMF sub-system then execute following command:
     `setSSVIP <VIP>`
     Where <VIP> is VIP address of the xMF sub-system

5.3.3 Change IP Address XMF subsystem in NSP

1. Login to the NSP GUI and navigate to **Centralized Configuration** Application
2. Navigate to **Equipment Registry** in Left Tree Panel
3. Click on **XMF ⊙ xMF Subsystem**
4. Modify the servers and change **Admin IP address** field to the new IP address
5. Check if the IP address and VIP address are correctly updated for xMF subsystem
6. Navigate to **Acquisition** in Left Tree Panel
7. **Apply Changes** on xMF
8. Verify that traffic is properly received by IXP

5.4 IXP Subsystem IP Change Procedure

This procedure describes how change the IP settings on the IXP subsystem.

Use this procedure in following cases:

- Server/Subsystem IP change
- Netmask change
- Default gateway change

This procedure uses the /root/bulkconfig file as an input of the changed IP addresses. User must be familiar with this file before executing this procedure.

Note: This procedure must be run via ILO

1. **Update the bulkconfig file**

a. Login to the iLO as root of any IXP server in the subsystem you are about to reconfigure

b. Update the `/root/bulkconfig` file with the new IP addresses

2. **Run IP change procedure**

a. Run the IXP subsystem IP change procedure as root:

```
# bc_changeip_subsystem.sh
```

b. The IXP subsystem healthcheck procedure will be triggered.

c. If the healtcheck procedure will end with no errors then the script will automatically continue with the IP change procedure. If there will be errors you will be asked for confirmation if you want to

continue. You can continue, but on your own risk. There is NO GUARANTEE that the system will be functional after and that the rest of the procedure will pass.

d. If you migrate the IXP subsystem in a scope of a single network the script will run until the end and there is no additional operation needed.

e. Perform any hardware related configuration like cabling etc.

f. Log in to the server where you have previously updated the bulkconfig file as `root` and run:

```
# bc_changeip_subsystem.sh --finish
```

Wait until the procedure finishes. Check for any errors. In case of any errors contact the Tekelec Customer Care Center

3. **Change IXP subsystem IPs in NSP**

a. Login to the NSP GUI and navigate to **Centralized Configuration** Application

b. Navigate to **Equipment Registry** in Left Tree Panel

c. Click on **IXP ⊙ IXP Subsystem**

d. Modify the servers and change **Admin IP address** field to the new IP address

4. **Change IXP subsystem's VIP in NSP**

a. Login to the NSP GUI and navigate to **Centralized Configuration** Application

b. Navigate to **Equipment Registry** in Left Tree Panel

c. Click on **IXP**

d. Modify the subsystem and change **VIP Address** field to the new IP address

e. Click Modify

5. **Apply changes**

a. Navigate to the **Mediation** view

b. Navigate to **Sites**

c. Open **IXP** and right-click on the subsystem.

d. Select **Apply changes…** from the popup menu.

e. Click on the **Next** button

f. Click on the **Apply Changes** button.

g. Wait until changes are applied.

h. Verify that result page does not contain any errors.

5.5 DWS IP Change Procedure

This procedure describes how change the IP settings on the DWS.

Use this procedure in following cases:

- Server IP change
- Netmask change
- Default gateway change

This procedure uses the /root/bulkconfig file as an input of the changed IP addresses. User must be familiar with this file before executing this procedure.

Note: This procedure must be run via ILO

1. **Update the bulkconfig file**
   a. Login to the iLO as root othe DWS server you are about to reconfigure
   b. Update the `/root/bulkconfig` file with the new IP addresses

2. **Run IP change procedure**
   a. Run the DWS subsystem IP change procedure as root:
   ```
   # bc_changeip_subsystem.sh --pre
   ```
   b. Continue with:
   ```
   # bc_changeip_subsystem.sh --change
   ```
   c. Continue with:
   ```
   # bc_changeip_subsystem.sh --post
   ```
   d. Finalize the IP change procedure on the DWS, as cfguser:
   ```
   $ makeDWH.sh
   ```
   Confirm, enter passwords where needed.

3. **Change DWS IP in NSP**
   a. Login to the NSP GUI and navigate to **Centralized Configuration** Application
   b. Navigate to **Equipment Registry** in Left Tree Panel
   c. Click on **DWS ⊙ DWS Pool**
   d. Modify the DWS and change **Admin IP address** field to the new IP address

4. **Apply changes**
   a. Navigate to the **Mediation** view
   b. Navigate to **Sites**
   c. Open **IXP** and right-click on the subsystem.
   d. Select **Apply changes…** from the popup menu.
   e. Click on the **Next** button
   f. Click on the **Apply Changes** button.
   g. Wait until changes are applied.
   h. Verify that result page does not contain any errors.

6 PIC Hardware Migration Procedures

6.1 Replace NSP Server

Note: This describes for example how to migrate the HP DL360 G6 servers to HP DL360 Gen8 servers.

1. **Take Backup**
   Take Backup of NSP Database Backup and Realm Backup
2. **Replace physically old server by new one**
3. **Perform Disaster Recovery on server**
   After replacing with new Gen8 hardware, perform disaster recovery on this box using NSP Disaster Recovery Procedures

6.2 Replace IXP Server

Note: This describes for example how to migrate the HP G6 servers to HP Gen8 servers.

Thus it's assumed that the IXP subsystem has already been upgraded to release 10 prior executing this procedure.

This procedure will guide you through the following highlevel steps:

- Backup the KPI sessions
- Integrate new server to IXP subsystem
- Offload old server to new server
- Remove old server from IXP subsystem
- Import KPI sessions on IXP subsystem

1. **Backup the KPI sessions on NSP**
   Note: Backup all the KPI sessions that need to be persisted after the hardware migration.

a. Open a web browser and log in to the NSP application interface.
b. Click on ProTrace application.
c. Select the session you want to backup. Run query on this session to get all requested KPIs. Then in the query result window click on Export.
d. Select either All Results or First x records options.
e. Enter a filename where these records will be exported. Choose Export type as ZIP.
f. Press Export and choose the location where you want to store this file. Then the zip file will be stored.
g. Repeat steps c-for each KPI session you want to backup.

2. **Integrate new server to IXP subsystem**

a. Run PIC installation procedure for IXP. Refer to **Installation document**, section IXP APPLICATION INSTALLATION PROCEDURES
b. Add this server to IXP subsystem that contains the old server you are about to replace.

3. **Offload old server to new server**
   From NSP GUI move all DFPs assigned to old server to new server.

4. **Put IXP old xDR Storage server to read-only mode**

   Note: This step is applicable to DWS server only.

   a. Open a web browser and log in to the NSP application interface.
   b. Navigate to **Mediation ⊙ particular IXP subsystem ⊙ Storage**
   c. The list of DWS Servers will be displayed.
   d. Mark the IXP old DWS server as `QUERY_ONLY`.

5. **Disable old PDU Storage server write permission**

   Note: This step is applicable to PDU Storage server only.

   a. Open a terminal window and log in to IXP old PDU Storage server as `root` user:
   b. Enter the platcfg menu. As `root` run:

```
# su - platcfg
```

   c. Navigate to **IXP Configuration ⊙ PDU Storage** and press **Edit**.
   d. Mark no both PDU Storage paths to disable writing. Press **OK**
   e. Leave the platcfg menu.

6. **Wait until IXP old server has no valid data**

   Wait as long as old server has any valid data. Once the session expired (in case of DWS server), or PDUs will be purged (in case of PDU storage server) you can continue with the rest of the procedure.

7. **Remove IXP old server from the IXP subsystem**

   The whole old IXP server functionality has been now replaced with new server. Remove the old IXP server from the IXP subsystem.

8. **Import KPI sessions to IXP subsystem**

   Note: Now you can import all the KPI sessions you have exported before the replacement. Run this step to any KPI session you need to import. The import of ZIP archive file is done by the IxpImport process. Only Oracle data are imported from .CDR file of the archive (PDU are ignored). Data are evenly distributed in the storage pool as in normal insertion by "IxpStore" process. If necessary, missing partitions are created during import.

   a. Open a web browser and login to the NSP application interface. Verify in CCM that all KPI sessions to local drive via scp.
   b. Open a terminal window and login to added G6 server as `cfguser`. Copy all zipped KPI sessions to local drive via scp.
   c. Import KPI session. As `cfguser` run:

```
$ IxpImport file session
```

   Where *file* is a full path including filename to zip file with particular KPI session and *session* is the session name that must already exists in CCM configuration.

   Output template:

```
Archive file: <file> Display configuration parameter summary. Pool name:
<pool_name>
Storage servers:
-ixpNNNN-XY ixp/ixp@<ip>/ixp
-ixpNNNN-XY ixp/ixp@<ip>/ixp
-ixpNNNN-XY ixp/ixp@<ip>/ixp
```

```
-ixpNNNN-XY ixp/ixp@<ip>/ixpDisplay pool information and storage server
list. Start import…
5% completed
10% completed
15% completed
…
90% completed
95% completed
Import completed
Display import progression. Progress information is based on:
(number of imported records * records size) / CDR file size. Begin time:
DD/MM/YYYY HH:MM:SS (GMT<+/-n>)
End time: DD/MM/YYYY HH:MM:SS (GMT<+/-n>)
Record count: xxxxxDisplay result information. Begin and end time are
displayed
 with local time zone.
```

6.3 HP G5 to Gen 8 migration

Refer to TR007444 Migration Guidelines G5 to Gen8- 10.0

7 NSP Maintenance Procedures

7.1 NSP Backup Procedures

NSP backup procedures protect the NSP system against the data loss and enables further data recovery during disaster recovery procedure.

7.1.1 Automatic Backup

7.1.1.1 Activate Automatic NSP Backup

This procedure describes how to activate the automatic backup procedure.

The backup procedure is activated automatically at the time of NSP installation. Automatic activation is performed using the cron task. The user can verify if the automatic backup is activated and if not then activate it by with this procedure.

1. **Verify if the backup is activated**

a. Login as `root` on NSP One-Box server or NSP Primary WebLogic server (Four-Box) - all following commands are executed as root

b. Check the cron job list

```
# crontab –l
```

Example of output when backup is already activated:

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

Here the backup procedure (`LaunchExpNSPdp.sh`) is scheduled for 22:00 (10:00 PM) every day

Example of output when backup is not activated:

```
no crontab for root
```

If no crontab is activated for `root`, then continue with the next step to activate the backup.

2. **Activate backup**

Run the following commands as root:

```
# cd /opt/nsp/scripts/oracle/cmd
# crontab crontab.nsp
```

3. **Verify if the backup is activated and functional**

a. Backup files are stored in the `/opt/oracle/backup/` directory on a daily basis on the NSP One-Box server or NSP Oracle server (Four-Box). Each subdirectory contains a timestamp of the backup.

```
drwxrwxrwx 2 root root 4096 Jul 13 22:00 NSP_BACKUP_07_13_09_22_00_00
```

b. For an NSP One-Box setup the directory structure is:

NSP_BACKUP_TIMESTAMP containing:

- A log file. It contains any information useful to troubleshoot a backup error.
- Database dump and log
- LDAP backup
- System files backup.

c. In the case of four box setup, the NSP_BACKUP dir will contain 4 sub- directories, one for each server of NSP Four-Box setup. Each of those directories will contain a backup of particular server.

The directory structure is:

- A log file. It contains any information useful to troubleshoot a backup error.
- NSP Oracle subdirectory contains:
  - Database dump and log
  - System files backup particular to the oracle server
- NSP Primary WebLogic subdirectory contains:
  - LDAP backup
  - System files backup particular to the primary server
- NSP Secondary WebLogic subdirectory contains:
  - System files backup particular to the secondary server
- NSP Apache subdirectory contains:
  - System files backup particular to the apache server

7.1.1.2 Deactivate Automatic NSP Backup

This procedure describes how to deactivate automatic NSP backup.

a. Login as `root` on NSP One-Box server or NSP Primary WebLogic server (Four-Box) - all following commands are executed as root

b. Check the cron job list

```
# crontab -l
```

If the output contains a record for LaunchExpNSPdp.sh then continue with the next step to remove this record. If the output does not contain a record for **LaunchExpNSPdp.sh** then the backup is not activated.

c. Edit the contents of the crontab

```
# crontab -e
```

Search for the entry in the crontab activating **LaunchExpNSPdp.sh** and remove it. Then save the changes to the crontab file.

Example: If the contents of the crontab file was following:

```
# crontab -l
00 22 * * * . $HOME/.bash_profile; cd     /opt/nsp/scripts/oracle/cmd; sh
./LaunchExpNSPdp.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
```

Then after modification, the output of the following command will be:

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

7.1.1.3 Change Automatic NSP Backup Time and Location

Execute this procedure to change an automatic backup time or location

1. **Change Automatic NSP Backup Time**

a. Login as `root` on NSP One-Box server or NSP Primary WebLogic server (Four-Box) - all following commands are executed as root

b. Check the cron job list

```
# crontab –l
```

If the output contains a record for LaunchExpNSPdp.sh then continue with the next step to remove this record. If the output does not contain a record for **LaunchExpNSPdp.sh** then the backup is not activated.

c. Edit the contents of the crontab

```
# crontab –e
```

Search for the entry in the crontab activating LaunchExpNSPdp.sh and replace values of backup time with new values of backup time. Then save the changes to the crontab file.

Example: If the backup procedure has been scheduled for 22:00 every day then the crontab for automatic backup (**`LaunchExpNSPdp.sh`** record) will look like:

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

The first two fields denotes the backup time. If you have changed the backup time to 13:30 every day then the output will be following:

```
30 13 * * * . $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd; sh
./LaunchExpNSPdp.sh >../trc/cronNSP.log 2>&1
```

2. **Change Automatic NSP Backup Location**

a. To change the location of where the backup files are stored runs the following command. As `root` run:

b. Edit the **LaunchExpNSPdp.sh** file using a text editor. Replace any occurrence of `/opt/oracle/backup` with a different backup directory.

c. Save changes.

7.1.2 NSP Database Backup

This procedure describes different steps to be followed for taking logical backup of NSP Oracle database. It is useful to have this backup in case of restoring the setup need arising from upgrade failure.

1. Login as a `root` user on NSP Server (In case of Onebox configuration) or Oracle server (In case of fourbox configuration) - all following commands are executed as root
2. Create a directory having write permission for the Oracle user:

```
# mkdir /opt/oracle/backup
# chown -R oracle:oinstall /opt/oracle/backup
```

3. If you want to backup the Data Exported using xDR Browser then use the following commands:

```
# cd /opt/nsp/scripts/oracle/cmd
# ./ExpNSPdp.sh NSP/NSP NSP /opt/oracle/backup
```

Where*/opt/oracle/backup* is an existing directory with write access for oracle user where the backup file will be created.

This script has three parameters and constraints:

- Oracle connection string (NSP/NSP) must not be modified
- Schema name to export (NSP) must not be modified
- Destination directory for the generated dump file (full existing path on the server) Copy this file /opt/oracle/backup/ExpNSP.dmp to a external source.

4. If you do not want to backup the Data Exported using xDR Browser then use the following commands:

Note: Use the following steps to export all NSP schema except the table COR_EXPORT_FILE (that may contain an extremely large amount export data).

```
# cd /opt/nsp/scripts/oracle/cmd
# ./ExpNSPdpNoEXPT.sh NSP/NSP NSP /opt/oracle/backup
```

Where /opt/oracle/backup is an existing directory with write access for oracle user where the backup file will be created. Copy this file /opt/oracle/backup/ExpNSPNoEXPT.dmp to an external source.

7.1.3 Realm Backup

This section describes the various steps and methods for performing a backup of Realm data.

1. Login as `root` user on NSP One-Box or NSP Primary WebLogic server (Four-Box)
2. Execute following commands to take back up. As `root` run:

```
# cd /opt/nsp/scripts
# cp -u
/usr/TKLC/nsp/nsp-
package/framework/install/dist/install/post_installation/LaunchExpNSPrealm.s
h
 /opt/nsp/scripts
# mkdir /opt/nsp/realmbackup
# ./LaunchExpNSPrealm.sh /opt/nsp/realmbackup
```

3. Verify the backup exist in /opt/nsp/realmbackup. Now backup this directory to an external media.
   Note: In case the script is run on NSP Primary WebLogic server, the backup will be stored on NSP Oracle server under the same directory `/opt/nsp/realmbackup`

7.1.4 System Files Backup

This procedure describes the various steps and methods for performing a backup of System data.

1. Login as `root` user on NSP One-Box or all NSP server (Four-Box)
2. Execute following commands to take back up. As `root` run:

```
# cd /opt/nsp/scripts
# ./ExpNSPSys.sh backup_directory
```

Where *backup_directory* is any directory with write access for root user where the backup file will be created. In the case of a four box setup, files will save in that box itself. Copy these files to an external source.

7.2 Start NSP Service on Primary when Secondary Is Down

This procedure is used to start NSP service on four box setup when Secondary box is down

1. Login as `tekelec` user on NSP Primary WebLogic server (Four-Box)
2. Execute following commands to start NSP service. As `tekelec` run:

```
$ cd /opt/nsp/bea/user_projects/domains/tekelec
$ sh startNSPPri.sh
```

7.3 Start NSP Service on Secondary when Primary Is Down

This procedure is used to start NSP service on Secondary box setup when Primary box is down

1. Login as `tekelec` user on NSP Secondary WebLogic server (Four-Box)
2. Execute following commands to start NSP service. As `tekelec` run:

```
$ cd /opt/nsp/bea/user_projects/domains/tekelec
$ sh startNSPSec.sh
```

7.4 Configure Apache HTTPS Certificate (Optional)

This procedure describes how to configure the Apache HTTPS certificate.

This procedure is optional; however, it is required when operating in a secured network environment and is available only on the NPS One-box or the Apache server (Four-box).

1. Login as `root` user on NSP One-Box or all NSP server (Four-Box)
2. Enter the **platcfg** menu. As `root` run:

```
# su - platcfg
```

3. Copy the files `server.crt` and `server.key` that are provided by the customer to `/root`.
4. Select **NSP Configuration ⊙ Configure Apache HTTPS Certificate**.
5. Press **Enter**.
6. Select **Yes** to confirm the action.
7. Exit the **platcfg** menu.

7.5 Copy NSP Backup

1. **Copy NSP Backup**

   Login to local machine which will be used to copy the nsp backup. Execute following command from the local machine

```
local_system_prompt>scp -r backup@nsp-ip:/path/to/backup/dir
local_backup_dir
```

- It will ask for backup user password, enter the password for backup user and press ENTER.
- **nsp-ip** should be replaced by the NSP backup server's IP address (NSP Server or NSP Oracle server in case of NSP 4-box configuration).
- */path/to/backup/dir* should be replaced by exact path of backup on server. For example*/opt/backup/backup/NSP_BACKUP_09_13_11_22_00_01*
- To note exact path of the backup you can use steps mentioned in step 2 below.

- *local_backup_dir* should be replaced by a directory name of the Customer choosing.
- After successful completion of the command the backup should be available at the *local_backup_dir* folder.
- In case of any error contact Tekelec Customer Care Support

2. **Note down the path of the backup folder on NSP server.**

a. Login as `root` on NSP One-Box server or NSP Oracle server (Four-Box)

b. Note the path of the backup to be copied by executing the command below:

```
tekelec$  ls -ld /opt/backup/backup/NSP_BACKUP*
```

It should output something like:

```
drwxrwxrwx 5 root root 4096 Sep  7 22:25
/opt/backup/backup/NSP_BACKUP_09_07_11_22_00_01
drwxrwxrwx 5 root root 4096 Sep  8 22:26
/opt/backup/backup/NSP_BACKUP_09_08_11_22_00_01
drwxrwxrwx 5 root root 4096 Sep  9 22:25
/opt/backup/backup/NSP_BACKUP_09_09_11_22_00_01
drwxrwxrwx 5 root root 4096 Sep 10 22:25
/opt/backup/backup/NSP_BACKUP_09_10_11_22_00_02
drwxrwxrwx 5 root root 4096 Sep 11 22:26
/opt/backup/backup/NSP_BACKUP_09_11_11_22_00_01
drwxrwxrwx 5 root root 4096 Sep 12 22:28
/opt/backup/backup/NSP_BACKUP_09_12_11_22_00_01
drwxrwxrwx 5 root root 4096 Sep 13 22:26
/opt/backup/backup/NSP_BACKUP_09_13_11_22_00_01
```

Where for example /opt/backup/backup/NSP_BACKUP_09_13_11_22_00_01 is the absolute path of the backup generated on 13th Sep 2011

Note: The name of folder is in format NSP_BACKUP_mm_dd_yy_hr_ms_sc, which denotes the date and time the backup was generated.

Note: If you want to backup the Alarm export file ,note the path of the file by using steps (c) and use in step1 (replace this path by /path/to/backup/file)

c. Backup Alarm export file menu. As `tekelec`, run following command on NSP (Oracle) Server

```
tekelec$ ls -lf /opt/backup/backup/ALA_*
```

It should output something like:

```
/opt/backup/backup/ALA_2011_07_01.csv
/opt/backup/backup/ALA_2011_07_12.csv
/opt/backup/backup/ALA_2011_07_23.csv
/opt/backup/backup/ALA_2011_07_02.csv
/opt/backup/backup/ALA_2011_07_13.csv
/opt/backup/backup/ALA_2011_07_24.csv
/opt/backup/backup/ALA_2011_07_03.csv
/opt/backup/backup/ALA_2011_07_14.csv
/opt/backup/backup/ALA_2011_07_25.csv
```

The File is in ALA_yyyy_mm_dd.csv format, note down the path of the file you wish to backup. For example /opt/backup/backup/ALA_2011_07_25.csv is the path for the Export file generated on the 25th of July 2011

7.6 EPI and Plugin Configuration for Tracing

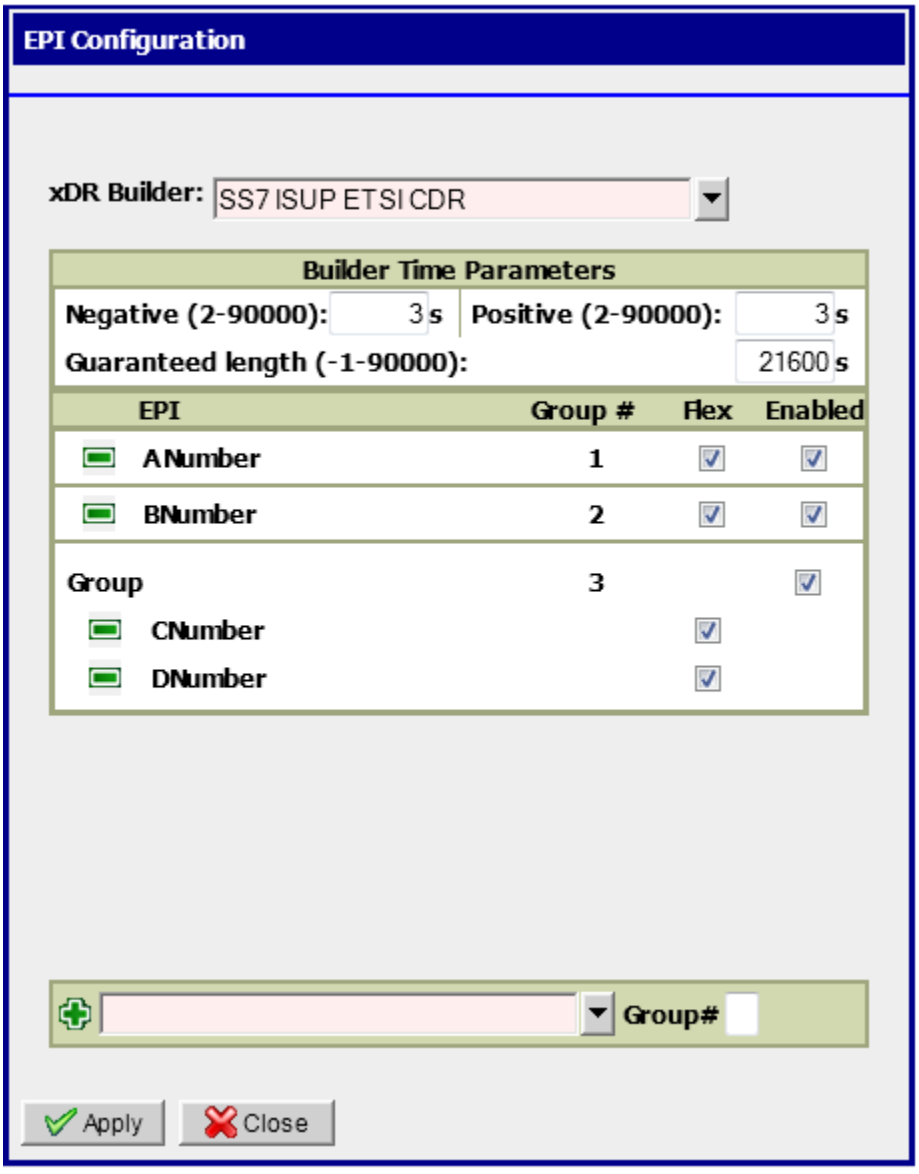
7.6.1 EPI Configuration

a) From Internet Explorer, connect to the NSP Application GUI using the following URL:
http://nsp_ip/nsp
Where nsp_ip is the IP address of the NSP One-Box server or NSP Primary WebLogic server (Four-Box).

b) Login with user `TklcSrv`
c) `Launch ProTrace Application from Applications`

7.6.1.1 Configuring Builder Time Tolerance Parameters

a) From Application Menu, Select Configuration > EPI. The EPI Configuration screen opens.
b) Select a builder from the pull-down menu. The screen changes to show the parameters for that builder.



c) Fill in the Builder Time Parameters.

The Builder Time Parameters define the time range used for searching for new xDRs. This time range is related to BEGIN TIME and END TIME of discovered xDRs and uses a Positive and a Negative value. The ranges for both positive and negative rules are 2-90000 seconds.

The Guaranteed length parameter allows you to enhance the search period to END_TIME + Guaranteed length. This parameter is used for search optimization and corresponds to the longest call or transaction the system is guaranteed to find.

d) Click on Apply to Save. The Builder Time Tolerance parameters would be saved successfully.

7.6.1.2 Add EPI

a) Open the EPI Configuration UI and Select a Builder. As in Section 9.8.1.1, a) and b)
b) Define the EPI's and EPI parameters for that builder.

EPI Name – Select any dictionary field from the drop down.

Group Number – Specify the group number in which you want to add EPI. If group number is blank then the default Group Number during Add operation would be the Max Group Number + 1 (max for the selected builder

c) Click Add button. The EPI will get added in the list.
    - Flex and Enabled would be checked by default
d) Click Apply. The changes are saved.

7.6.1.3 Delete EPI

a) Open the EPI Configuration UI and Select a Builder. As in Section 9.8.1.1, a) and b)
b) Click on delete button corresponding to EPI which you want to delete.
c) Click on Apply button.
d) The new configuration would be saved.

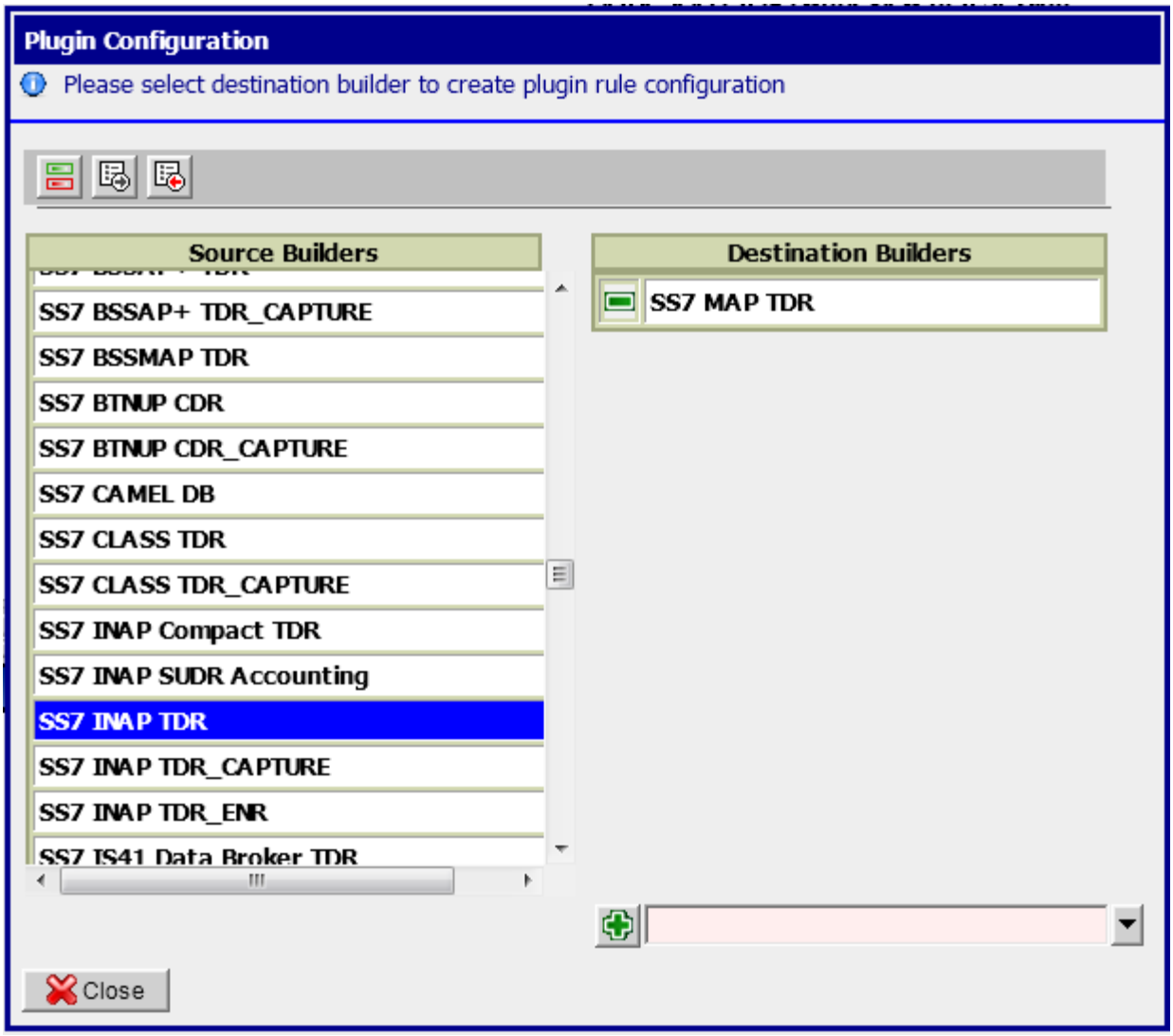
7.6.1.4 Update EPI

a) Open the EPI Configuration UI and Select a Builder. As in Section 9.8.1.1, a) and b)
b) Select (or de-select), the EPI parameters for that protocol.
    - Flex - defines whether the "Flex matching" is used for given field (see **Error! Reference ource not found.**Enabled - enabling/disabling the particular field as EPI
c) Click Apply. The changes are saved.

7.6.2 Configuring Plugins

7.6.2.1 Create Plugin

a) From Application Menu, Select Configuration > Plugins. The Plugin Configuration screen will be displayed.

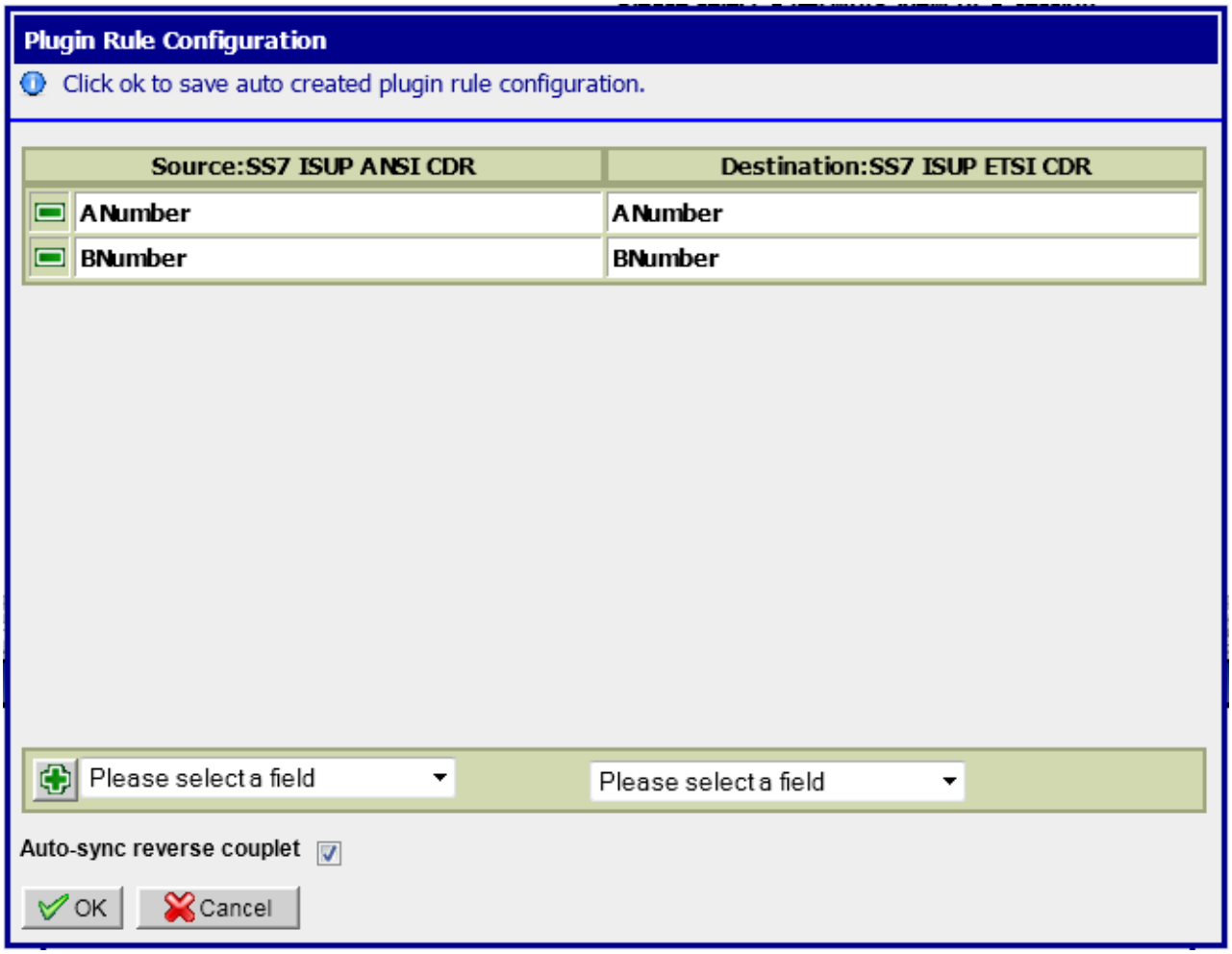


b) Click on Source Builder to configure. In the right pane all builders mapped with this source builder are populated.

c) To add a new plugin, select the destination builder from the available builders drop down

d) Click on Add Button

e) Plugin Rule Screen will open



f) Auto created Plugin Rules for the selected source and destination builders will get displayed. Auto Creation is done for the EPI's which are common to both the builders e.g. if ANumber is an EPI for both Source and Destination Builder a Plugin Rule ANumber → ANumber will be auto created in GUI.

g) If some auto created rules are not required, user can optionally delete them

h) If some more rules are required to be added user can optionally add more rules

i) The Auto-sync reverse couplet Check Box if checked would create a plugin in reverse directionas well when the Plugin is saved

j) Click on Add Button to create a Plugin Rule after selecting Source and Destination Fields

k) Click on Ok to Save the Configuration. Plugin would be created.

7.6.2.2 Update Plugin

a) From Application Menu, Select Configuration > Plugins. The Plugin Configuration screen will be displayed.

b) Click on Source Builder to configure. In the right pane all builders mapped with this source builder are populated.

c) Click on the Destination Builder to Edit Plugin

d) Plugin Rule Screen will be opened

e) Add/Delete required Plugin Rules

f) Click on Ok Button.

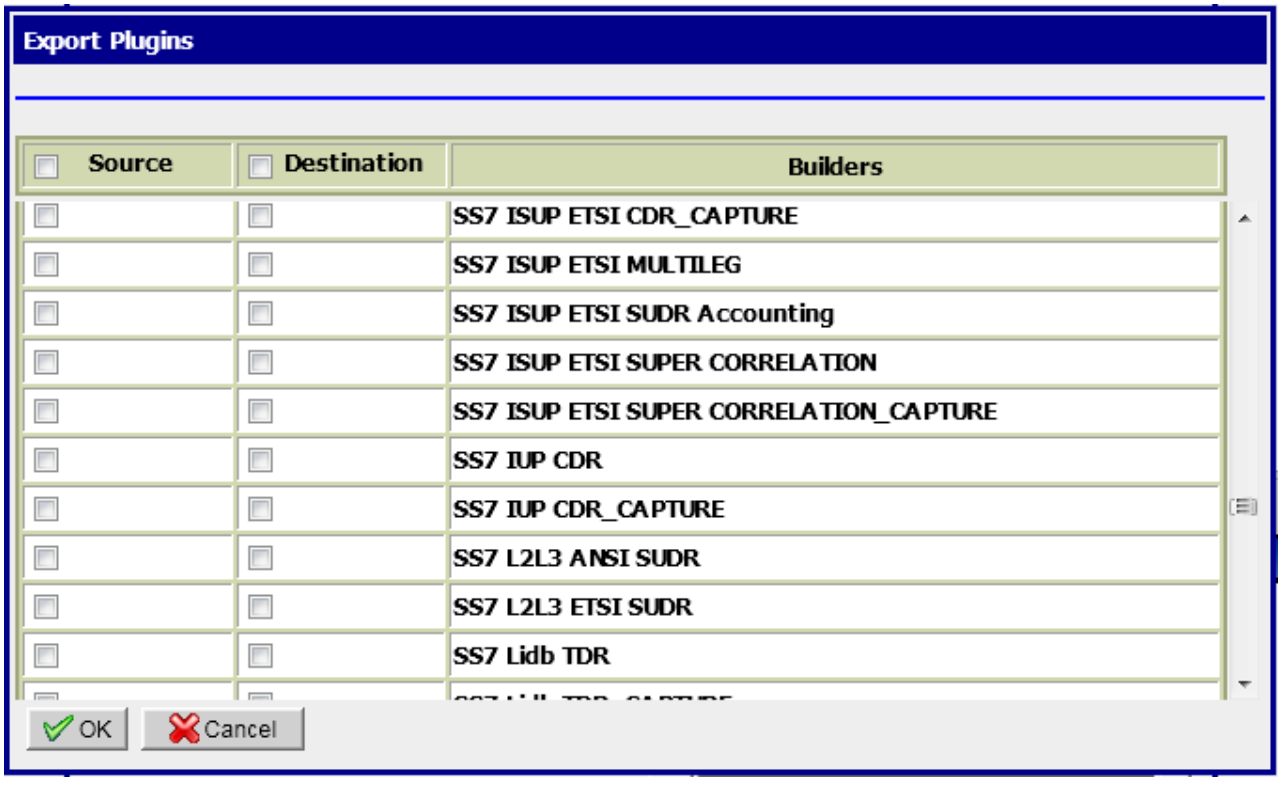
g) Plugin would be updated with new rules

7.6.2.3 Delete Plugin

a) From Application Menu, Select Configuration > Plugins. The Plugin Configuration screen will be displayed.
b) Click on Source Builder to configure. In the right pane all builders mapped with this source builder are populated.
c) Click on Delete Icon against the Destination Builder for the Plugin to be deleted
d) Click on Ok in the Warning Dialog Box
e) Plugin would be deleted and the list would be refreshed

7.6.2.4 Export Plugin Configuration

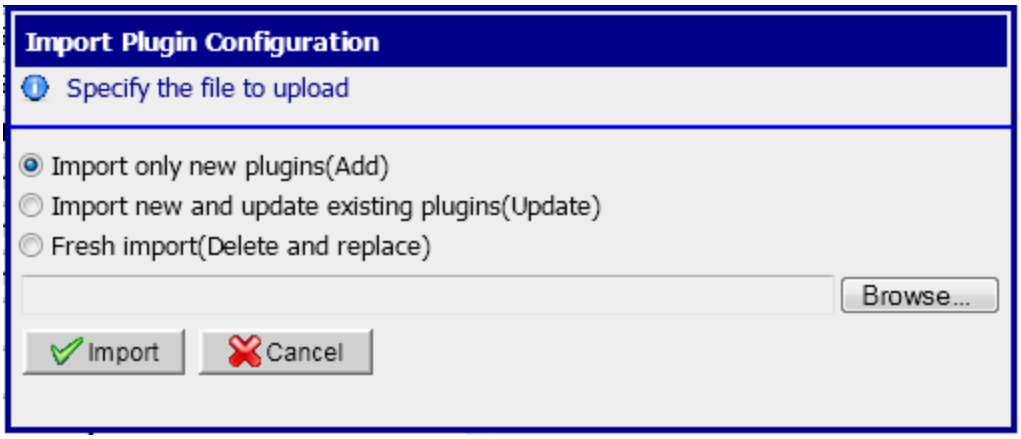
a) From Application Menu, Select Configuration > Plugins. The Plugin Configuration screen will be displayed.
b) Click on Export Button in the Toolbar
c) Export Plugin Screen will be opened
d) Select the Source and Destination Builders for which Plugin Configuration is to be exported. Check Source Check Box to export all plugins where this builder is a Source Builder. Check Destination Check Box to export all plugins where this builder is a Destination Builder.
e) Click on Export
f) Plugin Configuration for the checked source and destination builders is exported



7.6.2.5 Import Plugin Configuration

7.6.2.5.1 Using GUI

a) From Application Menu, Select Configuration > Plugins. The Plugin Configuration screen will be displayed.



b) Click on Import Button in the Toolbar
c) Import Plugin Configuration Screen will be opened
d) Select an Import Option to specify how the Plugin Configuration should be imported.
   - Select 'Import only new plugins(Add)' Option if you want to Import only those plugins from the csv file which are not already in the system
   - Select 'Import new and update existing plugins(Update)' Option if you want to Import all Plugins which are only in csv and not in database and update the plugins which are both in csv and database. Plugins which are only in database and not in csv would not be changed.
   - Select 'Fresh Import(Delete and replace)' Option to clean the database and Import all the plugins from the csv file
e) Browse the csv file
f) Click Import
g) Plugins would be imported according to the selected option

7.6.2.5.2 Using ant target

a) Login to nsp-primary box using tekelec user

```
tekelec$   cd /opt/nsp/nsp-package/protrace

tekelec$   ant import.plugin.rules -Dparam.import.file.name=<import file path> -
Dparam.import.type=<import type> -Dparam.create.epi=<create epi flag>
```

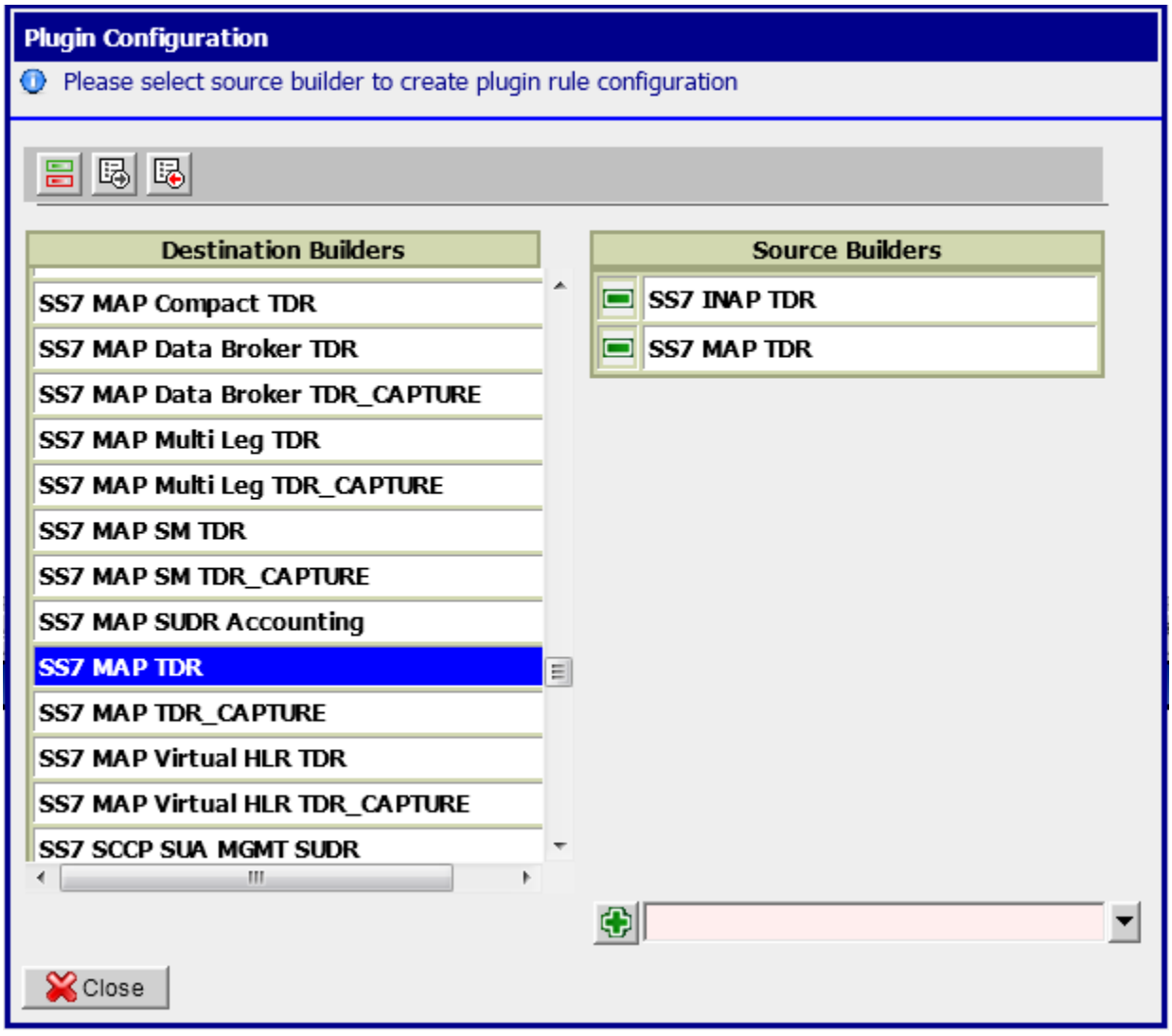
where,
<import file path> is the path of the CSV File to Import
<import type> is the Import Option as described in previous section,

- 0 represents Add
- 1 represents Update
- 2 represents Delete and Replace

<create epi> "Yes" if EPI Creation is required for missing EPI's. If it is set to "NO", Plugin Rules will not be created for missing EPI's

7.6.2.6 Toggle View Option 'Switch between Source and Destination View'

a) From Application Menu, Select Configuration > Plugins. The Plugin Configuration screen will be displayed.
b) Click on Toggle Button in the Toolbar
c) The Plugin Display View will change from Source → Destination to Destination → Source
d) Plugins and Plugin Rules can be Added/Deleted/Updated as explained, but the view display in this case will be Destination Builder → Source Builder for Plugins and Destination EPI → Source EPI in case of Plugin Rules. There will be no change in the software behavior except the view.



8 xMF Maintenance Procedures

8.1 Procedure to enable timestamp resolution to nanoseconds

This procedure describes how to enable/disable the timestamp resolution to ns on transport for IPRaw packet between PMF and IXP.
By default, this feature is disabled and the default timestamp resolution is the millisecond.
This feature can be activated separately for MFP or DTS transport protocol by the parameter '**TlvDsMask**' inside the '**LongParam**' table:

```
Yes|TlvDsMask|0|Set the XMF output interface mode (1-TLV_MFP_IP, 2-TLV_DTS_IP, 3-Both)
```

After modification of this parameter, the PMF must be restarted.

Note: A clobber on the xMF disable automatically this feature.

8.2 Falco Firmware upgrade procedure

Use the Document WI006872 at the end of the procedure, displayed version must be:

```
Version:  1.00i
FPGA V5:  C3090111
          0F120005
FPGA V4:  C1072711
          0F121E04
```

8.3 Key exchange procedure with Neptune probe

This procedure must be applied after a fresh install or upgrade of the Neptune probe.
It must applied on NSP servers for NSP 1 box and on both Primary WebLogic and Secondary WebLogic servers in case of NSP 4 boxes

These are the steps to follow (step 2 and 3 must be run for each Neptune probe)

1. Login as root on the NSP server
   a. Create the file containing the key
   b. Run the command :

```
$ /usr/TKLC/nsp/nsp-package/proadmin/scripts/retreive-cert.sh x.x.x.x > /tmp/neptune.crt
```

   x.x.x.x is the administration IP address of the Neptune probe
2. Import of the key
   a. Run the command :

```
$ export WL_HOME=/usr/TKLC/nsp/bea/wlserver_10.3
$ keytool -importcert -trustcacerts -alias x.x.x.x  -file /tmp/neptune.crt -keystore $WL_HOME/server/lib/DemoTrust.jks
```

   x.x.x.x is the administration IP address of the Neptune probe
   For Password : enter '*DemoTrustKeyStorePassPhrase*'
   Answer *Yes* when it is asking if the certificate is reliable
3. Restart the server
   a. In case of NSP 4 boxes, the following command must be run only when the steps below were applied on all WL servers
   b. Run the command (for NSP 4 boxes, run this command only on the Primary WebLogic server):

```
$ service nspservice restart
```

Remark *:* If the certificate is already present, the import must be deleted.

For deleting the import

1. Run the command *:*

```
$ export WL_HOME=/usr/TKLC/nsp/bea/wlserver_10.3
$ keytool –delete –keystore $WL_HOME/server/lib/DemoTrust.jks -alias x.x.x.x -
storepass DemoTrustKeyStorePassPhrase
```

   x.x.x.x is the administration IP address of the Neptune probe
2. Remove the file Neptune.crt under /tmp
3. Rerun import (step 2 and 3 above)

8.4 Add New Server in the IMF sub-system

The procedure should be executed for the IMF sub-system in case there is a need to add an additional server in the IMF sub-system. Following steps must be executed for adding the server in the already installed IMF sub-system:

1. Install IMF server
   a. **Install** the additional IMF server using the procedures mentioned in Chapter 5 in PIC Installation document,E53508-01.docx. Only procedures till section 5.3 should be executed. **Note: Use the bulkconfig file already present on the already installed servers and add the entry for the additional IMF server in the bulkconfig file. Copied the modified bulkconfig file to all the other IMF servers.**
2. Discover the server on NSP
   a. **Log in to the NSP application**
      i. Log in as tekelec to the NSP application interface using the NSP apache or one box server IP address.
      ii. Click **Centralized configuration.** The NSP application launches.
3. Discover the server on NSP
   a. **Modify IMF site on NSP**
      i. Select **Equipment Registry ► Sites**
      ii. Navigate to **XMF**
      iii. Right click in the requested subsystem
      iv. Select **Add** from the popup menu.
      v. Fill in the **Host IP Address** field with the IP address of the server you want to add.
      vi. Click the **Create** button.
      vii. Return to the **Equipment registry**.
      viii. Click on the subsystem to display the list of servers. Choose the newly added server and press **Discover applications.**
4. Apply Configuration on IMF
   a. **Apply Changes on IMF site on NSP**
      i. Navigate to the Mediation view.
      ii. Navigate to Sites
      iii. Open XMF and right-click on the subsystem.
      iv. Select Apply changes… from the popup menu.
      v. Click on the Next button
      vi. Click on the Apply Changes button.
      vii. Wait until changes are applied.
      viii. Verify that result page does not contain any errors.

9 IXP Maintenance Procedures

9.1 Offload DFPs from the IXP Server

This procedure describes how to offload the dataflow processing from the IXP server.

1. Redistribute processes

a) Open a web browser and log in to NSP application interface.
b) Click on **Centralized Configuration**.
c) Navigate to **Mediation**. Select the IXP subsystem and navigate to **IXP subsystem ⊙ Distribution**.
d) From the displayed table go to the **Server** column and redistribute processes from the offload server to the remaining servers.
e) Right click on the IXP subsystem in the **Mediation** menu and press **Apply changes**.

2. Redistribute DataFeed

a) Navigate to NSP home page
b) Click on **DataFeed**.
c) Open the **DataFeeds** tree and select **xDR/KPI exports**.
d) Deactivate all the processes that are assigned to the particular server by clicking on **Deactivate.**
   Wait until feed is deactivated.
e) If possible click on **Edit** button and redistribute such processes on the other servers by choosing new **Host name** and clicking on **Finish**.
f) If the **Edit** button won't be visible (in the case that feed status will be **Unknown** or **Recovering**) click on **Copy feed** and create a new feed with the same behavior on the new server. As soon as possible remove the old feed by **Delete** button.

3. Cancel KPI historical tasks

a) Go to the NSP home page
b) Navigate to the **ProTraq** application in the NSP.
c) Open **Historical task** tab.
d) Cancel all the tasks that are assigned to the particular server.

4. Reassign external connections

Note: The steps before take care about the stream tracking and if a producer dataflow processing has moved to another server, the consumer dataflow processing will finish processing the buffered data on the first server and automatically reconnect on the newly assigned server. But this automatic procedure does not apply to external connections.

a) Acquisition probe (IMF, PMF, MSW) sending data to a stream on this machine.
   In such a case it is required to reconfigure also this system in order to reconnect to the replacement (in general the spare) server
b) Other IXP subsystem processing output data from this subsystem.

This situation can be automatically managed if you configured two source IP addresses in the external Stream the consumer subsystem will find a new connection point to the data. If you did not assign a second IP address, you must edit the stream configuration and change the hostname or IP address of this stream accordingly

c) Queries: If the relevant server was used as the server answering to the queries, the subsequent connections will fail until this server has finished its maintenance.

If this period will be long, you must configure a new address for queries.

9.2 Enable/Disable Legacy Feed

This procedure describes how to enable/disable the legacy feed types. The legacy feeds are by default hidden in NSP GUI. This procedure will guide you how to show/hide them.

1. To enable the legacy feeds

Open a terminal window and log in on the NSP One-Box server or Weblogic Primary server (Four-Box setup) as tekelec. As `tekelec` run:

```
$ cd nsp-package/datafeed
$ ant legacyfeed.enable
```

2. To disable the legacy feeds

Open a terminal window and log in on the NSP One-Box server or Weblogic Primary server (Four-Box setup) as tekelec. As `tekelec` run:

```
$ cd nsp-package/datafeed
$ ant legacyfeed.disable
```

9.3 Convert feeds in backward compatible mode

a) Open a terminal window and log in as `tekelec` user on the NSP One-Box server or NSP Primary WebLogic server (Four-Box).

b) To convert the feeds to have an output in the backward compatible mode:

```
$ cd /opt/nsp/scripts/datafeed/
$ ./convertToBackwardCompatibleMode.sql
```

9.4 Configure Sessions for the Legacy Fixed Format xDRs Feed

This procedure describes how to configure the xDR session for the Fixed Format xDRs feed. This procedure is irreversible. Once this procedure is applied to the session the session can't be exported with the xDR/KPI feed. The only possibility is to use the legacy Fixed Format xDRs feed. SEQUENCE_ID column is used in case of proper failover of Fixed Format xDRs datafeed.

Note: Execute this procedure on all xDR Storage Servers in a pool.

1. Check if the oracle session contains the SEQUENCE_ID column

Note: The SEQUENCE_ID column is used in case of the proper failover of Fixed Format xDRs feed.

a) Open a terminal window and log in on the IXP xDR Storage server as `cfguser`.

b) As `cfguser` run:

```
$ sqlplus IXP/IXP@localhost/IXP
> desc session_name;
```

Where *session_name* is the case sensitive name of the source xDR session for feeding.

c) List of the columns defined for the session will be displayed.
Check whether it contains the SEQUENCE_ID column. In case that desired session has not a SEQUENCE_ID continue the procedure.

2. Enable SEQUENCE_ID

a) Open a web browser and log in to NSP application interface.
b) Click on **Centralized Configuration**.
c) Navigate to **Mediation ⊙ Sites ⊙ "site" ⊙ IXP ⊙ "subsystem" ⊙ Sessions**
d) Mark up the desired session and click on **Modify Session.**
e) A new page will display. Navigate to **Sequence Id**
f) Click on **Enabled**.
g) A popup window will display. Click **Ok**.
h) Click on **Modify**.

3. Check if the SEQUENCE_ID column has been created

a) In **Centralized Configuration** application navigate to **Mediation ⊙ Sites ⊙ "site" ⊙ IXP ⊙ "subsystem" ⊙ Sessions.**
b) In the list of the session find your session and check the **Sequence Id** column. **Enabled** should be marked.
c) Open a terminal window and log in back on the IXP xDR Storage server.

As `cfguser` run:

```
$ sqlplus IXP/IXP@localhost/IXP
> desc session_name;
```

Where *session_name* is the case sensitive name of the source xDR session for feeding. A list of columns defined for this session will appear. Column **SEQUENCE_ID** must be present now.

9.5 Configure PDU Storage Parameters

a) Log into any server from IXP subsystem
b) As `cfguser` run:

```
$ iqt -phz -f_name -f_role DaqServer
```

Example output:

```
ixp7000-1a StbMaster
ixp7000-1b ActMaster
ixp7000-1c Slave
```

The output will show you information about ActMaster and StbMaster of the subsystem
c) On ActMaster server, type:

```
$ ivi SubsystemTaskParam
```

The content of the table will be displayed, for example:

```
#!/bin/sh
iload -ha -xU  -fID -fParamName -fParamValue SubsystemTaskParam \
<<'!!!!!'
1|AlarmClear|1500
2|AlarmFail|1500
3|MaxFileAge|864000
4|MaxPercentUsage|90
5|ExcludePath|write.enable
```

```
6|Path|/opt/TKLCixp/pdu
7|Interval|5
8|Interval|300
9|Path|/es
10|ExcludePath|statistics
11|LoginName|ixp
13|AlarmFail|100
14|AlarmClear|100
15|OracleMaxPurgeTime|900
16|IdbPurgeTime|21600
17|TaskPurgeTime|604800
18|ExcludePath|run
19|DatabaseName|ixp0008-1a_DWH
20|HostName|ixp0008-1a
21|Password|IXP
!!!!
```

Change the value of parameter MaxFileAge (864000 seconds, in this example).
Don't forget to save the change when quitting the editor.

d) The table SubsystemTaskParam will be automatically replicated on all other servers of the subsystem. But you need to kill the process IxpPurge on each server of the subsystem so that the change is taken into account by the software.

```
$ pm.kill IxpPurge
```

Using command pm.getprocs, check that the process is actually restarted.

9.6 Enable/disable Write Access to the PDU Mounts

This procedure describes how to enable/disable write access to a specific PDU mounts. This procedure is applicable to IXP PDU storage servers.

1. To disable writing

a) Open a terminal window and log in on the IXP PDU Storage server as `root`. Enter a platcfg menu. As `root` run:

```
# su - platcfg
```

b) Navigate to **IXP Configuration ⊙ PDU Storage** and press **Edit**

c) Mark both PDU mounts to **no** to disable writing.
Note: After this step the IxpBuild processes will not be able to write to its PDU mounts from a specific PDU Storage Server. But mount point as such will still be accessible.

2. To enable writing

a) Open a terminal window and log in on the IXP PDU Storage server as `root`. Enter a platcfg menu. As `root` run:

```
# su - platcfg
```

b) Navigate to **IXP Configuration ⊙ PDU Storage** and press **Edit**

c) Mark both PDU mounts to **yes** to enable writing.
Note: After this step the IxpBuild processes will be able to write to its PDU mounts from a specific PDU Storage Server.

9.7 Set Behavior Mode for DWS Server

This procedure describes how to set the behavior mode for a specific DWS Server that is part of the

xDR storage pool.

a) Open a web browser and log in to NSP application interface.
b) Click on **Centralized Configuration**.
c) Navigate to **Mediation ⊙ Sites ⊙ IXP subsystem**
d) Click on **Storage**.
e) In the list in the right choose one of the 3 possible states: **ACTIVE**, **MAINTENANCE**, **QUERY ONLY**.
f) Right click on the IXP subsystem and press **Apply Changes**.

9.8 Recover Accidentally Unplugged MSA

This procedure describes how to restore the MSA after you have unplugged the MSA while the IXP server was still running.

a) Plug MSA back to IXP server.
b) Turn the MSA power on.
c) Reboot the IXP server and wait until reboot will prompt for the following:

```
-Press F1, to continue with the logical drives Disabled.
-Press F2, to accept data loss and to re-enable logical drives.
```

d) Choose `<F2>` option and continue booting.

9.9 Re-Sync the IXP Configuration

This procedure describes how to synchronize the IXP configuration from the NSP. This procedure is applicable to the IXP ActMaster server.

1. Drop synchronization history on the IXP ActMaster server

Note: This step will drop the synchronization history and such during the next Apply Changes the whole configuration will be synchronized from NSP to IXP subsystem.

a) Open a terminal window and log in on the IXP ActMaster server as `cfguser`.
b) As `cfguser` run:

```
$ /opt/TKLCixputils/bin/misc_force_sync.sh --all
```

2. Run Apply Changes to IXP subsystem from NSP

a) Open a web browser and log in to NSP application interface.
b) Click on **Centralized Configuration**.
c) Navigate to the **Mediation** view.
d) Navigate to **Sites**
e) Open **IXP** and right-click on the subsystem.
f) Select **Apply changes…** from the popup menu.
g) Click on the **Next** button
h) Click on the **Apply Changes** button.
i) Wait until changes are applied.
j) Verify that result page does not contain any errors.

9.10 Add Server to the IXP Subsystem

This procedure describes how to add a server to the IXP subsystem. This procedure is a general overview of a complex procedure.

This procedure is applicable to the IXP:

- IXP Base Server
- IXP PDU Storage Server

Prerequisite: This procedure assumes that the IXP server has been already installed accordingly to PIC Manufacturing Installation document and such server has not been integrated to any other IXP subsystem yet. This procedure describes the post-manufacturing integration to IXP Subsystem.

1. Integration with the IXP subsystem

Note: This step assume user is familiar with IXP bulkconfig file and its usage.

a) Open a terminal window and log in on IXP server you are about to add to the IXP subsystem as `root`.

b) Update the `/root/bulkconfig` file.
Note: The easiest way how to update the bulkconfig file is to copy the bulkconfig file from any server of the target IXP subsystem. Store this file to new IXP server. Then add the `host` line with newly installed IXP server to the bulkconfig file. Check that the bulkconfig file on the additional IXP server now contains overall subsystem configuration information and also make sure that the bulkconfig files contains records far all servers in the subsystem including the newly added one.

c) Once your bulkconfig is valid run automated integration script:
WORKAROUND PR200932: If user manually edited the `/etc/hosts` file any time before (which he is never supposed to do), this `/etc/hosts` file may be locked and the following step will fail with this message:

```
>>> Error: Checkout of /etc/hosts failed" appears in log run as root
```

In this case run the following as `root`:

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

And repeat the step again.

Note: This step must be run on additional IXP server, the one where you have updated the bulkconfig file in previous step.

Run the following steps:

1. As `root` run:
```
# bc_customer_integration.sh --local
```
2. Once finished server will reboot.
3. Log in back to the same newly added server. As `root` run:
```
# bc_adjust_subsystem.sh
```

d) Run analysis to see if the subsystem has been adjusted properly. As `root` run:

```
# bc_diag_bulkconfig.sh -a
```

2. Install the xDR Builder package

An xDR builder package must be associated to the particular subsystem before running this

procedure. All servers in the subsystem must have the same xDR builders' package.

As `cfguser` run:

```
$ server_builder_installer.sh -f xdr_builder_rpm_filename
```

Where *xdr_builder_rpm_filename* is the name of the builder `*.rpm` package already uploaded in the NSP and associated to this subsystem.

3. Add server to existing IXP subsystem

a) Open a web `browser` and log in to NSP application interface.
b) Click on **Centralized Configuration**
c) Navigate to **Sites**
d) Navigate to **IXP**
e) Right click in the requested subsystem
f) Select **Add** from the popup menu.
g) Fill in the **Host IP Address** field with the IP address of the server you want to add.
h) Click the **Create** button.
i) Return to the **Equipment registry**.
Click on the subsystem to display the list of servers.
j) Choose the newly added server and press **Discover applications.**

4. Apply configuration to the IXP subsystem

a) Navigate to the **Mediation** view.
b) Navigate to **Sites**
c) Open **IXP** and right-click on the subsystem.
d) Select **Apply changes…** from the popup menu.
e) Click on the **Next** button
f) Click on the **Apply Changes** button.
g) Wait until changes are applied.
h) Verify that result page does not contain any errors.

5. Locate the latest site code file

a) Open a terminal window and log in `cfguser` on the IXP Active Master server.
b) Locate the `IxpSubsystemKey.data` file in the `/home/cfguser/` directory.
As `cfguser`, run:

```
$ ls -l
```

A list of files appears. The `IxpSubsystemKey.data` must be included on this list.
c) Check the timestamp of the file. If the file is older than the time when the last server has been added to the subsystem or if the file is missing, regenerate the file.
As `root`, run:

```
# service TKLCixp restart
```

d) Locate the IxpSubsystemKey.data file in the /home/cfguser/ directory again. As cfguser, run:

```
$ ls -l
```

The list of files must contain the correct `IxpSubsystemKey.data` file.

6. Verify license installation

a) Log in as cfguser on the IXP Active Master server.
b) Run:

```
$ IxpCheckLicense
```

c) Verify the output.

The information about the license should state that license is valid and that license type is not STARTUP. If the license type is STARTUP contact the Tekelec Customer Care Center.

9.11 Add IXP Server to the IXP Subsystem in NSP/CCM

This procedure describes how to add the IXP server to the IXP subsystem that is already configured in CCM. This procedure is applicable once per IXP server. Run this procedure in NSP GUI.

1. Add server to existing IXP subsystem

a) Open a web browser and log in to NSP application interface.
b) Click on **Centralized Configuration**
c) Navigate to **Sites**
d) Navigate to **IXP**
e) Right click in the requested subsystem
f) Select **Add** from the popup menu.
g) Fill in the Host IP Address field with the IP address of the server you want to add.
h) Click the Create button.
i) Return to the **Equipment registry**.

Click on the subsystem to display the list of servers.

j) Choose the newly added server and press **Discover applications.**

2. Apply configuration to the IXP subsystem

a) Navigate to the **Mediation** view.
b) Navigate to **Sites**
c) Open **IXP** and right-click on the subsystem.
d) Select **Apply changes…** from the popup menu.
e) Click on the **Next** button
f) Click on the **Apply Changes** button.
g) Wait until changes are applied.
h) Verify that result page does not contain any errors.

9.12 Remove Server from the IXP Subsystem

This procedure describes how to remove a server from an IXP subsystem.

Note: Remove one server after the other; execute the full procedure for each server to remove.

1. Offload the IXP server

Offload DFPs from the server you are about to remove from the subsystem. Refer to *Offload DFPs from the IXP Server*.

2. Shutdown the IXP server you want to remove from the IXP subsystem

Open a terminal window and log in to the IXP server you want to remove from the IXP subsystem.

Shutdown this server. As `root` run:

```
# poweroff
```

3. Remove the xDR builders from the IXP subsystem in NSP

Note: this step has to be run for the **last server only** of the IXP subsystem.

a) Open a web browser and log in NSP application interface.
b) Click on **Centralized Configuration**.
c) Navigate to **Mediation ⊙Sites ⊙IXP Site ⊙IXP ⊙IXP subsystem ⊙xDR Builders**.
d) In the toolbar, click the garbage can icon (Delete All) to delete all the xDR builders associated to this IXP subsystem.
e) Confirm the deletion by clicking **OK**.

4. Remove server from the IXP subsystem in NSP

a) Open a web browser and log in NSP application interface.
b) Click on **Centralized Configuration**.
c) Navigate to **Mediation ⊙ Sites ⊙ IXP Site ⊙ IXP ⊙ IXP subsystem ⊙ Servers**.
d) In the list of the servers displayed on the right side mark the server that you want to remove.
e) Click on **Delete**.
f) Right click on IXP subsystem and press **Apply changes.**
g) Wait until system reconfiguration.

This will remove the IXP server from the IXP subsystem.

5. Remove the server from bulkconfig and adjust the subsystem accordingly

Note: Run this procedure from ANY IXP server in the IXP subsystem BUT NOT from a server you are about to remove.

a) Open a terminal window and log in to any remaining IXP server in the subsystem as `root`.
b) From the bulkconfig file remove host line with the IXP server you want to remove from the IXP subsystem.
c) As `root` run:

```
# bc_adjust_subsystem.sh
```

d) Run analysis to see if the subsystem has been adjusted properly. As `root` run:

```
# bc_diag_bulkconfig -a
```

9.13 Installation of External Datawarehouse

This procedure describes how to adapt the customer Oracle server to the External DatawareHouse for either the DataExport feature (Oracle To Oracle feeds) or the Oracle streaming feeds.
The customer Oracle server that is dedicated to be an External Datawarehouse need to fulfill the following prerequisites:

- Oracle 10g or 11g must be installed
  Note: Take care of using the same Oracle Database release as the one running on the DWS (or internal DWH). If the DWS run Oracle Database 11g, use Oracle Database 11g for the external DWH; if the DWS run Oracle Database 10g, use Oracle Database 10g for the external DWH.
- Database instance must be created with login and password
- 4 tablespaces must be created:
  - data tablespace with name DATA_CDR
  - index tablespace with name DATA_IND
  - configuration tablespace with name DATA_CONF
  - log tablespace with name DATA_LOG

1. **Customer: Grant roles**

Note: This step must be provided by the customer DBA. The customer needs to grant the following rights to the user that is created for you. Substitute *user_name* with the exact user name that will perform the installation.

Run the following commands in Oracle console:

```
SQL> GRANT SELECT ON DBA_FREE_SPACE TO user_name;
SQL> GRANT SELECT ON DBA_DATA_FILES TO user_name;
SQL> GRANT SELECT ON DBA_SEGMENTS TO user_name;
SQL> GRANT CONNECT TO user_name;
SQL> GRANT CREATE TABLE TO user_name;
SQL> GRANT CREATE ROLE TO user_name;
SQL> GRANT CREATE SEQUENCE TO user_name;
SQL> GRANT CREATE PROCEDURE TO user_name;
SQL> GRANT CREATE TRIGGER TO user_name;
SQL> GRANT CREATE PUBLIC SYNONYM TO user_name;
SQL> GRANT GRANT ANY ROLE TO user_name;
SQL> GRANT GRANT ANY PRIVILEGE TO user_name;
SQL> GRANT DROP ANY TRIGGER TO user_name;
SQL> GRANT DROP ANY ROLE TO user_name;
SQL> GRANT DROP PUBLIC SYNONYM TO user_name;
SQL> GRANT ADMINISTER DATABASE TRIGGER TO user_name;
SQL> GRANT UNLIMITED TABLESPACE TO user_name;
SQL> GRANT ANALYZE ANY TO user_name;
SQL> GRANT EXECUTE ON DBMS_LOCK TO user_name;
SQL> GRANT EXECUTE ON SYS.DBMS_SHARED_POOL TO user_name;
SQL> GRANT SELECT ON DBA_JOBS TO user_name;
SQL> GRANT SELECT ON DBA_JOBS_RUNNING TO user_name;
SQL> GRANT EXECUTE ON DBMS_JOB TO user_name;
SQL> GRANT CREATE ANY DIRECTORY TO user_name;
```

2. **Create the schema**

From any IXP server, as `cfguser`, run:

```
$ cd /opt/TKLCixp/prod/db/schema/cmd
$ ./ReinitDTO_Ee.sh user/password@ip/sid tablespace_conf tablespace_log
```

Where *user* is the database user with granted roles, *password* is the user password, *ip* is the IP address of the External DataWarehouse server, *sid* is SID of the instance provided by customer, *tablespace_conf* is the name of the configuration tablespace (e.g. `DATA_CONF`) and *tablespace_log* is the name of the log tablespace (e.g. `DATA_LOG`)

Note: during the installation you may obtain ERRORs/WARNINGs related to the dropping of the tables/roles etc. These errors don't have to be concidered as an error in case of the first installation (in this case the objects doesn't exist and cannot be deleted).

3. **Post-installation check**

Check the trace files in the `trc` directory to verify there were no additional errors then expected in the previous step.

Verify you can access External DataWarehouse console. From any IXP server, as `cfguser`, run:

```
$ sqlplus user/password@ip/sid
```

Where *user* is the database user with granted roles, *password* is the user password, *ip* is the IP address of the External DataWarehouse server and *sid* is SID of the instance provided by customer. You must be able to log in to External DataWarehouse Oracle console.

Check if the `dataserversession` table is present in user schema. In Oracle console run:

```
SQL> desc dataserversession;
```

You should receive the output similar to the following:

```
NAME                    NULL ?   TYPE
--------------------------------------- -------- --------------
ID                      NOT NULL NUMBER
NAME                    NOT NULL VARCHAR2(30)
TYPE                    NOT NULL NUMBER(2)
DATASERVERID            NOT NULL NUMBER(6)
DICTIONARY              NOT NULL BLOB
BEGINTIME                        NUMBER
ENDTIME                          NUMBER
RECORDCOUNT                      NUMBER
AVERAGECDR                       NUMBER
USERINFORMATION                  VARCHAR2(255)
```

Quit Oracle console:

```
SQL> quit
```

4. Install package, procedures and tables for the External DatawareHouse / DataExport feature

Note: This step is required only if the external dataware house is use for data export (Oracle To Oracle feeds)**.**

At this point we have created a running DB instance with the DTO schema. Now we need to install the missing packages, procedures and tables that are used by DataExport application.

a) From any IXP server, as `cfguser`, run:

```
$ cd /opt/TKLCdataexport/prod/db/cmd
$ ./CreateTKLCPkg.sh user/password@ip/sid
$ ./CreateTKLCTab.sh user/password@ip/sid tablespace_conf
```

Where *user* is the database user with granted roles, *password* is the user password, *ip* is the IP address of the External DataWarehouse server, *sid* is SID of the instance provided by customer and *tablespace_conf* is the name of the configuration tablespace (e.g. `DATA_CONF`).

Note: during the installation you may obtain ERRORs/WARNINGs related to the dropping of the tables/roles etc. These errors don't have to be concidered as an error in case of the first installation (in this case the objects doesn't exists and cannot be deleted).

b) Optionally, install and enable Oracle nightly jobs. Check with the DBA before activating the jobs. From any IXP server, as `cfguser`, run:

```
$ cd /opt/TKLCdataexport/prod/db/cmd
$ ./NightlyJob.sh user/password@ip/sid
$ ./CreateDir.sh user/password@ip/sid directory
```

Where *user* is the database user with granted roles, *password* is the user password, *ip* is the IP address of the External DataWarehouse server, *sid* is SID of the instance provided by customer and *directory* is the full path of the existing logs directory.

Note: The log directory has to exist and it should be stored on the partition with the sufficient space.

5. Tune the External DatawareHouse / Oracle feeds feature

Note: This step is required only if the external dataware house is used for Oracle streaming feeds.

Optionally, install and enable nightly jobs. Check with the DBA before activating these jobs. From any IXP server, as `cfguser`, run:

```
$ cd /opt/TKLCixp/prod/db/tuning/cmd
```

```
$ ./CreateJobClass.sh sys/sys_password@ip/sid
$ ./SystemStats.sh sys/sys_password@ip/sid -i
$ ./TuningPackage.sh user/password@ip/sid -i
$ ./FlushSharedPool.sh sys/sys_password@ip/sid
$ ./ModifyMaintenanceWindow.sh sys/sys_password@ip/sid 2 4
```

On Oracle 10g only:

```
$ ./ManageSpaceAdvisor.sh sys/sys_password@ip/sid -d
```

Where *sys_password* is the sys password, *user* is the database user with granted roles, *password* is the user password, *ip* is the IP address of the External DataWarehouse server and *sid* is SID of the instance provided by customer.

6. **Revoke DBA role**
   At this step the customer DBA can revoke the DBA role granted in step 1.

9.14 Setup NFS Mount for DataFeed Application on Customer Provided Server

This procedure describes the steps how to setup the nfs mount for Data Export on the customer provided server.

In some cases, the customer did not get an Export Server added to the IXP subsystem, so the traditional method is still used. UID for cfguser is 2000. The customer must change the UID on their server to allow cfguser to mount and access the filesystem.

Note: UNIX like system is expected to be installed on customer provided server.

1. **Create `cfguser` user and `cfg` group**

   Note: Run this step on customer provided server. No exact steps are provided. This differs from system to system.

   - UID for cfguser must be 2000
   - GID for cfg must be 2000

2. **Create export directories**

   Note: Run this step on customer provided server.

   Open a terminal window and log in as `cfguser`. As `cfguser` run:

```
$ mkdir -p /es/es_1
$ mkdir -p /es/es_2
$ chmod -R 750 /es
```

   Make sure that the owner of these directories is `cfguser` and group `cfg`.

3. **Update the `/etc/exports` file**

   Note: Run this step on customer provided server.

   Add the following lines into the `/etc/exports` file

```
/es      ixp????-??(rw,async,no_root_squash,anonuid=-1)
/es/es_1 ixp????-??(rw,async,no_root_squash,nohide,anonuid=-1)
/es/es_2 ixp????-??(rw,async,no_root_squash,nohide,anonuid=-1)
```

4. **Restart the NFS service**

   Note: Run this step on customer provided server. This step might be platform dependant. Check before executing this step.

As `root` run:

```
# service nfs stop
# service portmap restart
# service nfs start
```

5. Update the `/etc/hosts`

Note: Run this step on customer provided server.

Add all the IXPs that will use this server as an export target into the `/etc/hosts` file. Only those machines that will be present in `/etc/hosts` file and will pass the ixp hostname mask will be able to use this server as an export server.

6. Configure the DataFeed Application (NSP)

Note: Run this step in DataFeed application (under NSP).

Follow with standard DataFeed configuration. Set export server IP to the IP of the machine you just configured, set remote filesystem to `/es/es_1` or `/es/es_2` and set remote directory to the desired directory name that will be created under /es/es_?/.

10 Plateform based Maintenance Procedures

10.1 PM&C Disaster Recovery

Refer to PM&C Disaster Recovery procedure in PM&C Disaster Recovery

10.2 Install Operating System on G6 Rackmount Servers

This procedure describes how to install the operating system on the HP DL360 and HP DL380 G6 rackmount servers.

For an estimated time for this procedure, refer to the applicable flowcharts in xMF Disaster Recovery Procedures.

Before you perform this procedure, make sure that you have the appropriate TPD DVD/CD or ISO File available. Refer to the topic Software Requirements.

Note: This procedure needs to be executed only for xMF G6 servers.
Note: This procedure describes a re-installation of Operating System in case of Disaster Recory procedure. The BIOS configuration procedures which have been already executed during the fresh installation are not described.

1. **Insert the TPD DVD/CD and reboot the server**

   The server should boot on the DVD/CD and display a `boot` prompt.

2. **Install the operating system**

   At the `boot` prompt, enter the appropriate installation parameters for the console:

   ```
   boot: TPDnoraid console=ttyS0 diskconfig=HWRAID,force
   ```

3. **Rebootthe server**

   After the installation process has completed successfully, the server prompts for a reboot. Click **Reboot**.

   If the installation did not complete successfully, contact the Tekelec Customer Care Center.

10.3 Install Operating System on Gen8 Rackmount Servers

Refer to installation of operating system procedure described in PIC Installation document

10.4 Install Operating System on E5-APP-B Servers

Refer to installation of operating system procedure described in Tekelec Platform Initial Product Manufacture Release 5.5 909-2229-001 Revision B

10.5 IPM Blade Servers Using PM&C Application

1. **IPM Servers Using PM&C Application**
   Refer to IPM procedure using PM&C application in Platform Configuration Procedure Reference
2. **Additional configuration step after IPM**

This step is mandatory on all blades server after IPM.

Some parameters must be commented out in file /etc/sysctl.conf

1. Connect as root user on the blade

2. Run

   # rcstool co /etc/sysctl.conf

3. edit file /etc/sysctl.conf (with e.g.)

   comment out (with "#" sign in first character of line) the 3 lignes starting with "net.bridge"

4. Run

   # rcstool ci /etc/sysctl.conf

10.6 Switch Disaster Recovery

Refer to APPENDIX: Switches Configuration in E53508-01 PIC 10 installation Procedure
Note: Take care to check in any customer specific config was applied

11 External Software Configuration

11.1 Java Runtime settings

User has to Configure workstation Java plug-in for some application:

1. Update to the latest JRE (version 7 update 51 or later)
2. Configure Runtime parameters
   - Go to Start Menu ➢ Control Panel ➢ Java
   - Select the Java tab and click on View button
   - Here, you will find Java Runtime parametersremove any memory parameter (-Xmx or –Xms)
3. As security rules have been enforced in order to run applets (ProAlarm config), configure Exception Site List in Security parameters
   - Go to Start Menu ➢ Control Panel ➢ Java
   - Select the Security tab
   - Click on Edit Site List ➢ Add
   - Enter NSP URL like **Erreur ! Référence de lien hypertexte non valide.**>

To apply new settings close the Browser and start it again in case application is already running

11.2 IE Browser Settings

This procedure describes the steps for making the settings in IE browser.

The below mentioned configuration must be done for the IE browser on the client side to access any of the NSP applications.

1. Force Refresh

a. Navigate to **Tools ⊙ Internet Options**
b. Select **General** Tab
c. Click on **Settings** button
d. Select radio button for Every visit to the page
e. Click on **OK**
f. Click on **OK** on Internet Options window.

2. **Scripting**
    a. Navigate to **Tools ⊙ Internet Options**
    b. Select **Advanced** Tab
    c. On **Browsing** part check the option **Disable script debugging**
    d. Uncheck **Display a notification about every script error**
    e. Click **OK** on Internet Options window

3. **Auto resize popup windows**
    a. Navigate to **Tools ⊙ Internet Options**
    b. Select **Security** tab
    c. Select **Internet zone**
    d. Click on **Custom level** button
    e. Set to **enable** to the parameter **Allow script-initiated windows without size or position constraint**
    f. Click **OK**

4. **Allow windows without address bar**

Setting needs to be done for IE7 only.

    a. Navigate to **Tools ⊙ Internet Options**
    b. Select **Security** tab
    c. Select **Internet zone**
    d. Click on **Custom level** button
    e. Set to **enable** to the parameter **Allow web site to open windows without address bar**
    f. Click **OK**

5. **Enable Downloads**
    a. Navigate to **Tools ⊙ Internet Options**
    b. Select **Security** tab
    c. Select **Internet zone**
    d. Click on **Custom level** button
    e. Set to **enable** all the settings under **Downloads** (i.e.set to enable the following parameters : *Automatic prompting for file downloads, File download, Font download*)
    f. Click **OK**

6. **Configure IE to have more than two download sessions**

    Note: **The steps below describe how to configure Microsoft Internet Explorer or Windows Internet** Explorer to have more than two download sessions.

    a. Navigate to Start ➢Run
    b. Type **regedit** and press <ENTER>
    c. Locate the following key in the registry:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings
```

    d. On the **Edit** menu point to **New**
    e. Click on **DWORD Value** and then add the following registry values:

```
Value name: MaxConnectionsPer1_0Server
Value data: 10
Base: Decimal

Value Name: MaxConnectionsPerServer
Value data: 10
Base: Decimal
```

f. Quit Registry Editor

7. Enable Active Scripting

a. Navigate to **Tools ⊙ Internet Options**
b. Select **Security** tab
c. Select **Internet zone**
d. Click on **Custom level** button
e. Set to **enable** the option **Active Scripting** under **Scripting**
f. Click **OK**

8. Download Hot Fix for GWT 1.4 compatibility issue on IE7

Note: This step need to be done for IE7 as NSP 4.1 supports IE 7 with hot fix

a. Go to *http://support.microsoft.com/kb/933873*
b. Click on **view and request hotfix downloads option**
c. Follow the instructions provided in the site and Download HotFix from there
d. Extract it
e. Install it

9. Enable Applet Table Format For ProTrace

Note: This step needs to be done if Applet Table format is required for Protrace.

a. Enable Java in Browser
   Navigate to *http://www.java.com/en/download/help/enable_browser.xml*
b. Follow the instructions provided in the site to enable java in the browser
c. Click **Enhanced Security**
d. Run the following for IE8
e. Navigate to **Tools ⊙ Internet Options**
f. Select **Advanced** Tab
g. On **Browsing** part check the option **Enable third-party browser extensions**
h. Click **OK**
i. Navigate to **Tools ⊙ Internet Options**
j. Select **Security** tab
k. Select **Security zone**
l. Adjust settings for this zone. Recommended is **Trusted Sites**

10. ActiveX Controls

a. Navigate to **Tools ⊙ Internet Options**
b. Select **Security** tab

c. Select **Internet zone**
d. Click on **Custom level** button
e. Set to **enable** the options
   - **Run ActiveX controls and plug-ins**
   - **Script ActiveX controls marked safe for scripting**
   - **ActiveX controls and plug-ins**
f. Click **OK**

11. Clear History

On Windows workstation open Internet Explorer and navigate to **Tools ⊙ Options ⊙ Delete**.

12. Compatibility view

Note: This step needs to be done for IE9

Some NSP application may not display correctly for the desktop, using **Compatibility View** might help. If Internet Explorer recognizes a NSP application that isn't compatible, you'll see the Compatibility View icon on the address bar

To turn on Compatibility View, click the Compatibility View button to the make the icon change from an outline to a solid color.

12 Knowledge Base Procedures

12.1 How to mount the ISO file via iLO

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

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

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

12.2 Configure and Verify ILO Connection

This procedure is applicable to all HP.

ILO is an independent subsystem inside a HP server, which is used for out of band remote access. This subsystem permits to monitor, power-off, and power-on the server through a LAN-HTTP interface. The setup of this device shows up during each power-on sequence of the server. When the message for ILO configuration is proposed, hit the <F8> key and follow the on-screen instruction. In case of no user action after a few seconds, the boot sequence continues to the next step. In this situation, it would be necessary to reboot the device to return to this choice.

Recommended configuration consists of assigning an IP address to the system and creates a “root” user. This setup needs to be done in accordance with the customer’s supervision environment.

Minimal steps are:

- Menu “Network”, “DNS/DHCP”, “DHCP enable”, change to OFF, save [F10]
- Menu “Network”, “NIC and TCP/IP”, fill-in the IP address, Subnet Mask, Gateway, Save [F10]
- Menu “User”, “Add user”, “User name” root, “Password”, < same-value-than-TPD >
- Menu “ File”, exit and save

For verification of the setup, connect the ILO interface to the network switch.

1. Open Internet Explorer on a workstation and enter in the ILO IP address.
2. You will get a SSL security warning
3. Accept the warning.

4. Once you are logged in click on Launch to start **Integrated Remote Console**
5. If you will receive another certificate warning click on **Yes** to continue
6. If you get the application's digital signature can not be verified click Always trust content from this publisher then click **Run**.
7. A remote console window will now appear to allow you to access the HP server.

12.3 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 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:

   - Insert the CD containing an iso image into the removable media drive of the PM&C server.
   - 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:
     - Go 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
       ```

   Note: Refer to the documentation provided by application for pmacftpusr password.

2. **PM&C GUI: Login**

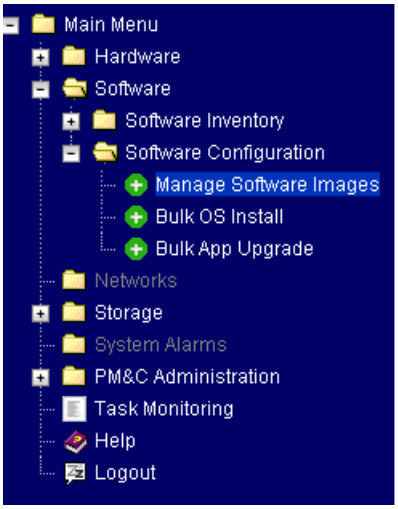
   - Open web browser and enter:

     ```
     http://<management_network_ip>/gui
     ```

   - Login as pmacadmin user

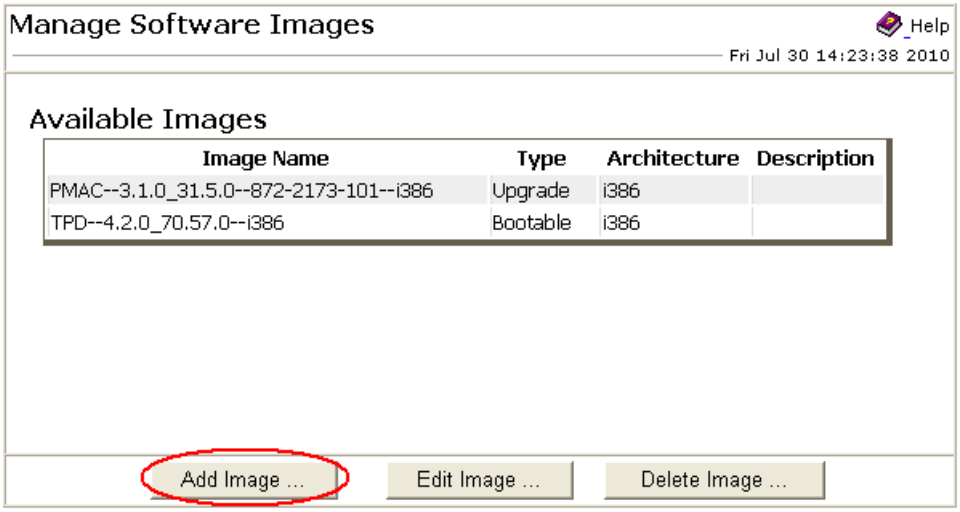
3. **PM&C GUI: Navigate to Manage Software Images**

   Navigate to **Main Menu ⊙ Software ⊙ Software Configuration ⊙ Manage Software Images**

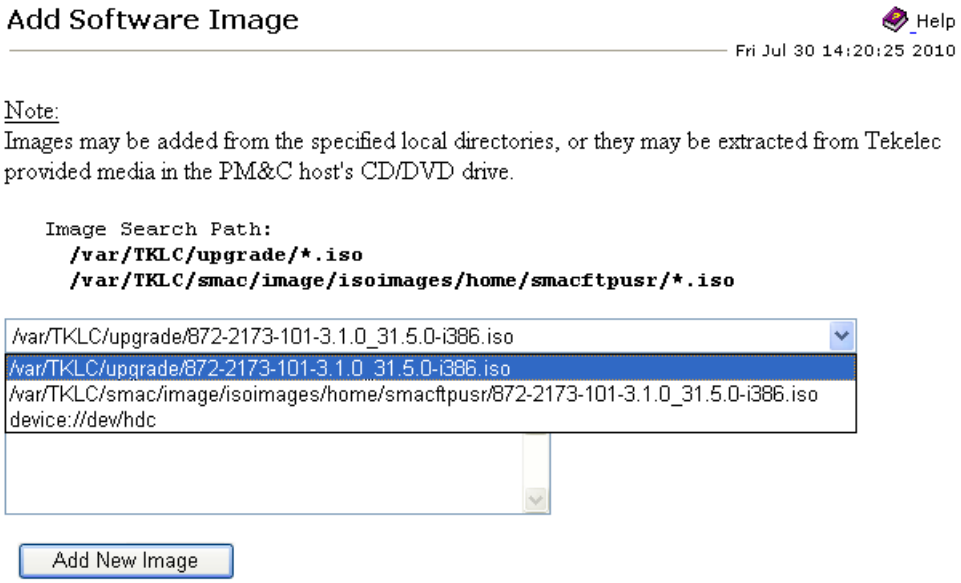
   

4. **PM&C GUI:Add image**

- Press the **Add Image** button.



- 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.



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

12.4 How to remove IP Address and Route

This procedure describes how to remove the IP address and Route on TPD

1. Remove IP address

```
# netAdm delete --address={ipaddress} --device={interface}
```

Where ***{interface}*** will be the interface needs to be removed, e.g eth02
Where ***{ipaddress}*** will be the IP address needs to be removed, e.g 172.22.49.10

2. Remove IP route

```
# netAdm delete --route=net --device={interface} --gateway={gw_ipaddress} --
address={net_ipaddress} --netmask={net_mask}
```

Where **{*interface*}** will be the interface needs to be removed, e.g eth02
Where **{gw_ipaddress}** will be the IP address of the gateway needs to be removed, e.g 172.21.48.250
Where **{net_ipaddress}** will be the IP address of network, e.g 172.20.48.0
Where **{net_mask}** will be the mask of network, e.g 255.255.254.0

3. Use ifconfig and route command to verify that the IP address and the route have been removed

12.5 How to recover OA board paswword

In case the OA default password paper tag is no more attached to the on the board and you need to recover the administrator password, follow this procedure:

1. Connect a serial console on the OA RJ45 port
2. Open a console using putty or Hyper Terminal
3. Press the OA reset button during 5s
4. While the OA restart press "L" to enter in the Lost password mode.
5. Finally password should be displayed

12.6 Security Requirement: Granting and revoking DBA role to NSP user

12.6.1 Revoke DBA role from NSP user after successful NSP installation on one box or oracle box (in case of four box system).

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

```
# su - oracle
```

2. Login to sqlplus console using command:

```
# sqlplus sys/oracle as sysdba
```

3. Check whether NSP has DBA role or not by executing below command:

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

If the output of command is same as shown above then execute below steps to revoke DBA role from NSP user but if DBA is not shown in the above list then skip the execution of below steps.

4. Execute command to revoke the DBA privilege from NSP user

```
# REVOKE DBA FROM NSP;
```

Below message will appear on the console after successful completion of the command.

```
Revoke succeeded.
```

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

```
# SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'NSP';
GRANTED_ROLE
```

```
------------
RESOURCE
CONNECT
```

If the result of above command is not the same as shown above and still contains DBA role in result set then please contact Oracle's Tekelec Customer Care Center.

12.6.2 Grant DBA role to NSP user after NSP is installed on one box or oracle box (in case of four box system).

1. Login to NSP machine and change user to oracle by command:
```
# su - oracle
```

2. Login to sqlplus console using command:
```
# sqlplus sys/oracle as sysdba
```

3. Check whether NSP has DBA role or not by executing below command:
```
# SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'NSP';
GRANTED_ROLE
------------
RESOURCE
CONNECT
```
If the output of command is same as show above then execute below steps to grant DBA role to NSP user but if DBA role is shown in the above list then skip the execution of below steps.

4. Execute command to grant the DBA privilege to NSP user
```
# GRANT DBA TO NSP;
```
Below message will appear on the console after successful completion of the command.
```
Grant succeeded.
```

5. Execute below command to confirm that DBA role has been granted to NSP user or not
```
# SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'NSP';
GRANTED_ROLE
---------------
RESOURCE
CONNECT
DBA
```
If the result of above command is not the same as shown above and still does not show DBA role in the result set then please contact Oracle's Tekelec Customer Care Center.

AppendixA. 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.

AppendixB. Locate Product Documentation on the Oracle Technology Network Site

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

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

2. Under Applications, click the link for Communications.

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

3. Click Oracle Communications Documentation for Tekelec Products.

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

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