Oracle® Communications Performance Intelligence Center

Maintenance Guide

Release 9.0

March 2014

ORACLE®

Oracle Communications Performance Intelligence Center Maintenance Guide, Release 9.0

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access Oracle's Tekelec Customer Support site and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

Refer to Error! Reference source not found. for instructions on accessing this site.

Contact Oracle's Tekelec Customer Care Center and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

Phone: 1-888-FOR-TKLC (1-888-367-8552) or 919-460-2150 (international)
FAX: 919-460-2126

CHANGE HISTORY

Date	Version	Author	Comments	Approved (Yes/No)
21/11/12	0.1	François Cêtre	Creation from 7.5 maintenance guide 909-2197-001 rev#30	No
21/11/12	0.2	François Cêtre	Various cleaning	No
23/11/12	0.3		Add chapter “Convert feeds in backward compatible mode” in IXP maintenance procedures	No
14/12/12	0.5	C. Stoeckel	PR 221163	No
19/12/12	0.6	A. Kiffer	PR 222403	No
08/01/13	0.8	P. Tribollet	PR 221795	No
15-jan-2013	0.9	JF Muller	PR 223082 – IXP server removal	No
15/01/13	0.10	S.Haegelin	Falco upgrade	No
16-jan-2013	0.11	JF Muller	PR 213491 – External DWH setup	No
14/02/2013	0.12	S.Haegelin	Remove section 2.11 and replace by 2.13	No
27/02/2013	0.13	Gaurav Agnihotri	PR#216858: Modified xMF IP change procedure, section 7.3 & 7.4	No
15/04/2013	1.0	S.Haegelin	Document presentation	Yes
16/04/2013	1.1	S.Haegelin	Referesh table of content	No
15/05/2013	1.2	JF Muller	PR 224154 –IXP healthcheck after DRed server has been reintegrated	No
15/05/2013	1.3	S.Haegelin	Update for 9.0.3	No
21/05/2013	1.4	S.Haegelin	Update for 9.0.3	No
24/05/2013	1.5	S.Haegelin	Update PDU Storage parameters configuration	No
13/06/2013	1.6	S.Haegelin	Typo correction	No
14/06/2013	1.7	S.Haegelin	Orange Fr DR	No
25/06/2013	1.8	S.Haegelin	Typo correction in section 11.12	No
26/06/2013	1.9	S.Haegelin	NSP4Box DR clarifications	No
24/07/2013	1.10	S.Haegelin	Add the procedure to recover from rommon prompt	No
26/07/2013	1.11	S.Haegelin	Add cisco link	No
29/07/2013	1.12	S.Haegelin	Updated the config register value to 2102 in section 16.9	No
30/07/2013	2.0	S.Haegelin	To take in account the new switch config	Yes
21/11/2013	2.2	C. Stoeckel	PR233615	No
30/01/2014	2.4	B. Chappell	Oracle re-branding of title & legal pages	No
25/02/2014	2.5	B. Chappell	Updated page 2 text	No
03/03/2014	2.6	B. Chappell	Corrected problems with Section 4.2	No
06/03/2014	2.7	S.Haegelin	Fixed hyperlink issues	No

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

HP Solutions Firmware Upgrade Pack 2.2 909-2234-001 Revision B, April 2013
PM&C 3x/4.x Disaster Recovery 909-1638-001 Rev B, September 2012
Platform 6.x Configuration Procedure Reference 909-2209-001 Revision E January 2013
EAGLE SW Compatibility Matrix SS005887 V15

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 Access the Customer Support Site (ESWD Download Center)

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a software. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the Tekelec Customer Support site (http://support.tekelec.com/ or https://secure.tekelec.com/OA_HTML/ibuhpage.jsp within Tekelec network).

Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Download Center** tab to access the software iso file.
3. Firmawares are available faor all customers under the name A-Tekelec Firmware Releases
4. The PIC product is availbale under the customer name.
5. To download a file to your location, right-click the file name and select **Save Target As**.

1.5 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

1.6 Requirements and Prerequisites

1.6.1 Hardware Requirements

PIC release 9.0 don't supports anymore TEK1 server.
For detailed information on the hardware supported refer to PIC 9.0 planning guide
http://signal.tekelec.com/Depts/salesmktg/ProductInformationLibrary/Forms/FeaturePlanningGuides.aspx

1.6.2 Software Requirements

The following software are required for the PIC 9.0 installation.

Note: For specific versions and part numbers, see the PIC 9.0 Release Notice.

IXP 9.0.0-x.x.x
Oracle DVD in BOM for 12 disk config
Oracle DVD in BOM for 24/25 disk config (fresh install or migration only)
NSP 9.0.0-x.x.x
Oracle 10.2.0.5 in BOM
Weblogic 10.3.5.0 in BOM
xMF 9.0.0 –x.x.x (TPD3)
xMF 9.0.0 –x.x.x (TPD5)
xDR Builder 9.0.0–x.x.x
TADAPT
MSW

ATM 155
SM – used with MSW
Report Server
Oracle DVD in BOM for 12 disk config
Oracle DVD in BOM for 24/25 disk config (fresh install or migration only)
BOE Fresh Install
BOE Upgrade
PPS
TDM Voice Analytics
Roaming Access
Roaming Data
Mobile Data
Sigtran Transport
SS7 Transport
Firmwares
HP SOLUTIONS FIRMWARE 2.2.1 or more
TPD Versions
TPD Linux XMF TEK1/TEK2
TPD Linux HP G5&G6&TEK3 (RMS&Blade)
PM&C
PM&C

1.6.3 Licenses Requirements

Licenses required for software installation of PIC 9.0 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 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.

a) Install the operating system.

- For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
- For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
- For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
- For C-class blade follow IPM Blade Servers Using PM&C Application

2. Mount oracle volume

Estimation: 10 min

- For C-class blade setup follow Remount NSP LUN
- For Rackmount servers follow:

a) Insert the NSP package CDROM.
b) Mount DVD/ISO.

As root run:

- For a DVD/CD, run:

```
# mount /media/cdrom
```

- For an ISO file, run:

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

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

c) As root run:

- For a DVD/ISO, run:

```
# sh iso_mount_point/scripts/mount_oracle_part.sh
```

iso_mount_point with the absolute path where the ISO is mounted e.g.: `/media/cdrom`

d) After successful execution of script unmount the cdrom. As root run:

As root run:

- For a DVD/CD, run:

```
# umount /media/cdrom
```

- For an ISO file, run:

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

3. NSP one box fresh install

Estimation: 70 min

a) Complete the installation by following the steps in section NSP Pre-Install Configuration and Steps for Install WebLogic, then Install Oracle Database and then Install NSP.

b) 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.

4. Check permission for backup directory

a) Execute following commands.

As root run:

```
# 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.

5. Restore the database and realm

a) Restore the realm by following Restore Realm Backup

b) Restore the oracle database by following the Restore Backup Using Import Utility.

6. Enable protrace tracing

Note: Protrace Tracing needs to be enabled using platcfg

menu. a) Login to platcfg menu

b) Go to **NSP Configuration ⊙ Configure optional applications**

c) Select **Edit** on this GUI.Select **ProtraceTracing** .

Use Arrowkeys for Navigation on GUI and “Spacebar” to select ‘Yes/No’ .Select ‘**Yes**’ to enable protrace tracing.

d) Enter **OK**

7. Reboot the server

a) Reboot the NSP server

8. Install A-Node on Server

a) Open a terminal window and log in on NSP Primary Web-Logic serveras root
b) Insert the XMF CD to the cdrom
c) If ISO is available copy the iso to NSP primary server at some location.
d) 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)
e) Type yes to confirm
f) No reboot need

NOTE (WORKAROUND PR 216438) :: - During Onebox Server Disaster recovery user need 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
```

2.2 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

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.

a) Install the operating system.

- For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
- For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
- For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
- For C-class blade follow IPM Blade Servers Using PM&C Application

2. Complete the NSP Apache installation

a) Complete installation by following the steps for NSP Pre-Install Configuration and then Install NSP for the the apache server installation .

3. Reboot the NSP Apache server

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.

a) Install the operating system.

- For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
- For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
- For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
- For C-class blade follow IPM Blade Servers Using PM&C Application

2. Mount oracle volume

Estimation: 10 min

- For C-class blade setup follow Remount NSP LUN.
- For Rackmount servers follow:

a) Insert the NSP package CDROM.
b) Mount DVD/ISO.

As root run:

- For a DVD/CD, run:

```
# mount /media/cdrom
```

- For an ISO file, run:

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

where *iso_path* is the absolute path of the ISO image, which includes the name of the image

(for example, `/var/TKLC/upgrade/iso_file_name.iso`).

c) As root run:

- For a DVD/ISO, run:

```
# sh iso_mount_point/scripts/mount_oracle_part.sh
```

iso_mount_point with the absolute path where the ISO is mounted e.g.: `/media/cdrom`

d) After successful execution of script unmount the cdrom. As root run:

- For a DVD/CD, run:

```
# umount /media/cdrom
```

- For an ISO file, run:

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

3. Install the oracle server

a) Complete the installation of the oracle server by following the steps in section NSP Pre-Install Configuration the steps for Install Oracle Database for Oracle Box Installation and Install NSP

4. Check permission for backup directory

a) Execute following commands.

As root run:

```
# 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.

5. Restore the oracle database

Restore the oracle database by following the Restore Backup Using Import Utility.

6. Reboot the NSP Oracle server

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.

a) Install the operating system.

- For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
- For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
- For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
- For C-class blade follow IPM Blade Servers Using PM&C Application

2. Complete the NSP Secondary WebLogic Installation

a) Complete the installation by following the steps in section NSP Pre-Install Configuration and the steps for Install WebLogic and Install NSP

3. Recover the Primary server

a) Recover the primary server by following the steps mentioned in Primary WebLogic (Four-Box)

4. Reboot the NSP Secondary server

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.

a) Install the operating system.

- For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
- For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
- For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
- For C-class blade follow IPM Blade Servers Using PM&C Application

2. Prepare server for recovery

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

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

b) As `root` run:

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

3. Restore optional modules files

a) 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_l
ist
 /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.

4. Complete the NSP Primary WebLogic Installation

a) Complete the installation by following the steps in section NSP Pre-Install Configurationand the steps for Install WebLogicand Install NSP

5. Enable protrace tracing

Note: Protrace Tracing needs to be enabled using platcfg menu.

a) Login to platcfg menu
b) Go to **NSP Configuration ⊙ Configure optional applications**
c) Select **Edit** on this GUI.Select **ProtraceTracing** .

Use Arrowkeys for Navigation on GUI and “Spacebar” to select ‘Yes/No’ .Select ‘**Yes**’ to enable protrace tracing.

d) Enter **OK**

6. Import the Realm

NOTE: - Backup used for restoring realm for Disaster recovery must be NSP Nightly Backup present at /opt/oracle/backup/ under NSP_BACKUP_XX folders

a) Restore the realm by following Restore Realm Backup

7. Reboot all the NSP cluster

a) Reboot all 4 NSP servers from the Four-Box setup

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

8. Install A-Node on Server

a) Open a terminal window and log in on NSP Primary Web-Logic serveras root
b) Insert the XMF CD to the cdrom
c) If ISO is available copy the iso to NSP primary server at some location.
d) 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)

e) Type yes to confirm
f) No reboot need

9. Restore SNMP and SMTP configuration

a) For SNMP, follow “Modify SNMP Agent IP Address (Optional)” chapter from 909-2241-001
b) For SMTP, follow “Configure Mail Server (Optional)” chapter from 909-2241-001

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

Login as tekelec user on NSP Server (NSP primary box in case of four box)

$ 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

2.3 Remount NSP LUN(C-class blades only)

This procedure describes different steps to follow to remount the logical volumes from MSA2012fc to NSP server after Disaster Recovery of one box server or Oracle
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**
   a) Login as **root** user on the NSP server for onebox setup or oracle server of a four box NSP.
2. **Retrieve LUN numbers of logical volumes**
   a) As root run:

```
# multipath –ll
```

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

Example:

```
mpath0 (3600c0ff000d5809fb180cc4901000000) dm-6 HP,MSA2012fc
[size=70G][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:0:37 sdc 8:32  [active][ready]
\_ round-robin 0 [prio=1][enabled]
```

```
\_ 1:0:0:37 sdd 8:48  [active][ready]
mpath1 (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc
```

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

b) The lun# is the 4th number in the 4th and 6th line of each block, here in the example **37** for mpath0, **36** for mpath1 and **35** for mapth2

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

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

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

3. Recreate mapping to SAN REDO volume

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

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

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

c) After completion, the output must show:

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

4. Recreate mapping to SAN DATA volume

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

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

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

c) After completion, the output must show:

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

5. Recreate mapping to SAN BACKUP volume

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

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

b) when prompted for **Login on Remote** with the user `platcfg`

c) After completion, the output must show:

```
<result>
```

```
1
</result>
```

6. Check the volume names

a) As root run:

```
root# multipath -ll
```

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

Example:

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

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

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

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

7. Check the file system

a) As root run:

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

8. Mount the volumes

a) As root run:

```
# mount -a
```

9. Verify the volumes

a) Actual values may change from example below:

df –h

```
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root
                     496M  123M  349M  26% /
/dev/cciss/c0d0p1    122M  9.9M  106M   9% /boot
none                 4.0G     0  4.0G   0% /dev/shm
/dev/mapper/vgroot-plat_tmp
                    1008M   47M  910M   5% /tmp
/dev/mapper/vgroot-plat_usr
                     4.0G  1.1G  2.7G  30% /usr
/dev/mapper/vgroot-plat_var
                     496M   40M  431M   9% /var
/dev/mapper/vgroot-plat_var_tklc
```

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

2.4 NSP Pre-Install Configuration

This procedure describes how to configure the NSP servers, which is required prior to installing 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 NSP 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. **Log in as root on the server that you want to install the application. As root user run:**

   ```
   # syscheck
   ```

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

   Example ouput for a healthy system:

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

   Running modules in class proc...
                                   OK
   ```

   ```
   Running modules in class system...
                                   OK

   Running modules in class hardware...
                                   OK
   ```

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

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

2. Create the bulkconfig file (or copy the file from an other server)

a) As a `root` user.
b) Create the `/root/bulkconfig` file.

3. Configure the server hostname

a) Enter the **platcfg**
menu. As `root`, run:

```
# su - platcfg
```

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

4. Configure SNMP

a) From the main **platcfg** menu, select **Network Configuration ⊙ SNMP Configuration ⊙ NMS Configuration** and select **Edit > Add A New NMS Server**.
b) Type the IP address as `127.0.0.1` and `TEKELEC` as the community string and port number is optional user can leave this field and then click **OK**.
c) Click **YES** to restart alarm server and then press any Key to
continue. d) Exit the **platcfg** menu.

5. Add the cdrom entry to /etc/fstab

a) Create the **cdrom**
folder. As `root`, run:

```
# cd /media
# mkdir cdrom
```

b) Take the backup of `/etc/fstab` file.
As `root`, run:

```
# cp -f /etc/fstab /etc/backup_fstab
```

where backup_fstab will contain the contents of file /etc/fstab

c) Edit the `/etc/fstab` file.
As `root`, run:

```
# rcstool co /etc/fstab
# echo "/dev/cdrom /media/cdrom auto pamconsole,exec,noauto,managed 0 0" >>
/etc/fstab
```

d) Compare the contents of `/etc/fstab` and `/etc/backup_fstab`.
As `root`, run:

```
# diff /etc/fstab /etc/backup_fstab
```

The output must contain the following line:

```
/dev/cdrom  /media/cdrom   auto    pamconsole,exec,noauto,managed 0 0
```

e) Check in the `/etc/fstab` file.
As `root`, run:

```
# rcstool ci /etc/fstab
```

f) Verify the entry in `/etc/fstab`.

As `root`, run:

```
# cat /etc/fstab
```

The output should include the following line:

```
/dev/cdrom   /media/cdrom    auto    pamconsole,exec,noauto,managed 0 0
```

2.5 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 DVD/CD or ISO file available.
- Verify the `/root/bulkconfig` file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.

Note: Run this procedure via iLO.

1. Log in and either insert the DVD/CD or distribute the ISO file

a) Log in as `root` on the server that you want to install WebLogic.

b) Distribute the media:

- On the rackmount server insert the WebLogic DVD/CD or mount the WebLogic ISO file via iLO (see How to mount the ISO file via iLO).
- On the c-class blade server download the ISO from the PM&C ISO repository. ISOs are available on the PM&C server under the `/var/TKLC/smac/image` directory. Store the ISO file to `/var/TKLC/upgrade` directory. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure Adding ISO Images to the PM&C Image Repository

2. Validate the installation media

a) Enter the **platcfg** menu. As `root`, run:

```
# su - platcfg
```

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

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

CDROM is Valid

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

d) Exit the **platcfg** menu.

3. Mount the media

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

- For a DVD/CD (rackmount server), run:

```
# mount /media/cdrom
```

- For an ISO mounted via iLO (rackmout server), run:

```
# getCDROMmedia
```

to check which CDROM device has been added to the `/dev/` directory. Example output:

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

This example output denotes virtual CD-ROM device `/dev/scd0`. Then mount this device to `/media/cdrom/` directory.

```
# mount -o loop virtual_cdrom_device /media/cdrom
```

where *virtual_cdrom_device* is the path to virtual CD-ROM device received in a previous step.

- For an ISO file (c-class server), run:

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

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

4. Install WebLogic

a) As `root`, run the appropriate command depending on the mount point used:

- For a DVD/CD or virtual CDROM, run:

```
# /media/cdrom/install_weblogic.sh
```

- For an ISO file, run:

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

b) Wait until the installation process is complete.

5. Unmount the media

a) As `root`, run the appropriate command depending on the mount point used:

- For a DVD/CD, run:

```
# umount /media/cdrom
```

- For an ISO file, run:

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

b) If the ISO file was copied to the server, then remove this file to save disk space. As `root`, run:

```
# rm -f /var/TKLC/upgrade/iso_file
```

where *iso_file* is the name of the ISO image.

6. Analyze the installation log

a) 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 Tekelec Customer Care Center.

b) Verify the size of the WebLogic product.

As `root`, run:

```
# du -sh /opt/nsp/bea
```

The result should be approximately 1.1G.

c) Verify the contents of the WebLogic installation.

As `root`, run:

```
# ll /opt/nsp/bea
```

Example of the output:

```
#
total 152
-rwxr-xr-x 1 tekelec tekelec    12 Mar  3 11:19 beahomelist
drwxr-xr-x 8 tekelec tekelec  4096 Mar  3 11:17 jdk160_18
drwxr-xr-x 7 tekelec tekelec  4096 Mar  3 11:17 jrockit_160_17_R28.0.0-679
drwxr-xr-x 2 tekelec tekelec 12288 Mar  3 11:19 logs
drwxr-xr-x 9 tekelec tekelec 49152 Mar  3 11:19 modules
-rwxr-xr-x 1 tekelec tekelec   624 Mar  3 11:19 ocm.rsp
-rwxr-xr-x 1 tekelec tekelec 59430 Mar  3 11:19 registry.dat
-rwxr-xr-x 1 tekelec tekelec  2074 Mar  3 11:19 registry.xml
drwxr-xr-x 8 tekelec tekelec  4096 Mar  3 11:19 utils
drwxr-xr-x 9 tekelec tekelec  4096 Mar  3 11:16 wlserver_10.3
```

2.6 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 DVD/CD or ISO file available.
- Verify the `/root/bulkconfig` file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.
- In case of c-class blades SAN Configuration must be done properly before starting Oracle Installation

.

Note: Run this procedure via iLO.

WORKAROUND PR196740: If the server changed its function or different version of Oracle was previously installed manually, clean up first ~1000MB of each partition using dd command before Oracle installation.

1. Log in and either insert the DVD/CD or distribute the ISO file

a) Log in as `root` on the server where you want to install the Oracle database.

b) Distribute the media:

- On the rackmout server insert the Oracle DVD/CD or mount the Oracle ISO file via iLO (see How to mount the ISO file via iLO).
- On the c-class blade server download the ISO from the PM&C ISO repository. ISOs are available on the PM&C server under the `/var/TKLC/smac/image` directory. Store the ISO file to `/var/TKLC/upgrade` directory. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure Adding ISO Images to the PM&C Image Repository

2. Validate the installation media

a) Enter the **platcfg** menu. As `root`, run:

```
# su - platcfg
```

b) Select **Maintenance ⊙ Upgrade ⊙ Validate**

Media. c) Select the desired upgrade media and press **Enter**.

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

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

d) Exit the **platcfg** menu.

3. Mount the media

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

- For a DVD/CD (rackmount server), run:

```
# mount /dev/cdrom /media
```

- For an ISO mounted via iLO (rackmout server), run:

```
# getCDROMmedia
```

to check which CDROM device has been added to the `/dev/` directory. Example output:

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

This example output denotes virtual CD-ROM device `/dev/scd0`. Then mount this device to `/media` directory.

```
# mount -o loop virtual_cdrom_device /media
```

where *virtual_cdrom_device* is the path to virtual CD-ROM device received in a previous step.

- For an ISO file (c-class server), run:

```
# mount -o loop /var/TKLC/upgrade/iso_file /media
```

where *iso_file* is the ISO filename.

4. Install Oracle

As `root`, run:

```
# /media/install_oracle.sh
```

Note: When installing Oracle 11g you will be prompted by the following:

```
You are about to install Oracle 11G and ASM. Are you sure you want to continue
(yes/no)
```

Type `yes` to confirm. Press `<enter>` to continue.

When the installation process is complete the server will automatically reboot.

5. Remove the ISO file.

a) After reboot open a terminal window and log back in as `root`.

b) If the ISO file was copied to the server, then remove this file to save disk space. As `root`, run:

```
# rm -f /var/TKLC/upgrade/iso_file
```

where *iso_file* is the ISO filename.

6. Analyze the installation log

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

If there are any errors, contact the Tekelec Customer Care Center.

2.7 Install NSP

This procedure describes how to install the NSP on a server with the operating system installed (TPD). Before you perform this procedure :

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

Note: Run this procedure via iLO.

1. Log in and either insert the DVD/CD or distribute the ISO file

a) Log in as `root` on the server that you are want to install the NSP application.
b) Distribute the media:

- On the rackmount server insert the NSP DVD/CD or mount the NSP ISO file via iLO (see How to mount the ISO file via iLO).
- On the c-class blade server download the ISO from the PM&C ISO repository. ISOs are available on the PM&C server under the `/var/TKLC/smac/image` directory. Store the ISO file to `/var/TKLC/upgrade` directory. If the ISO is not present in PM&C ISO repository add the ISO file using the procedure Adding ISO Images to the PM&C Image Repository

2. Validate the installation media

a) Enter the **platcfg** menu. As `root`, run:

```
# su - platcfg
```

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

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

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

d) Exit the **platcfg** menu.

3. Install NSP

a) Enter the **platcfg** menu. As `root`, run:

```
# su - platcfg
```

b) Select **Maintenance ⊙ Upgrade ⊙ Initiate Upgrade**. c) Select the upgrade media and press **Enter**.

The installation process launches. Wait until the installation process is complete.

d) If the ISO file was copied to the server, then remove this file to save disk space.

As `root`, run:

```
# rm -f /var/TKLC/upgrade/iso_file
```

where *iso_file* is the absolute path of the ISO image, which includes the name of the image.

4. Analyze the installation and upgrade logs

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 Tekelec Customer Care Center.

2.8 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

Restore Realm backup

a) Login as `root` on NSP server (for One-box or DIH NSP setup)or NSP Primary WebLogic server
(Four-Box).

b) Copy the realm backup into a local directory.

As `root` run:

```
# 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.

c) 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

As `root` run:

```
# 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/`)

2.9 Restore Backup Using Import Utility

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`.
In case of all boxes recovery make sure you completed all the steps and the 3 other server are operational.

Note: In 4-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 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+w <DIR_CONTAINING_DUMP>
```

- 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

a) Import scripts

They 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

1. Login as “root” user on NSP Server for One box or on Primary server for four box and run the command

```
# service nspservice stop
```

2. Login as `root` user on NSP Server for one-box or Oracle Server for four box

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

- ```
  # cd  /opt/nsp/scripts/oracle/cmd
  ```
- ```
  # ./RestoreDatabase.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**).

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

possible errors.

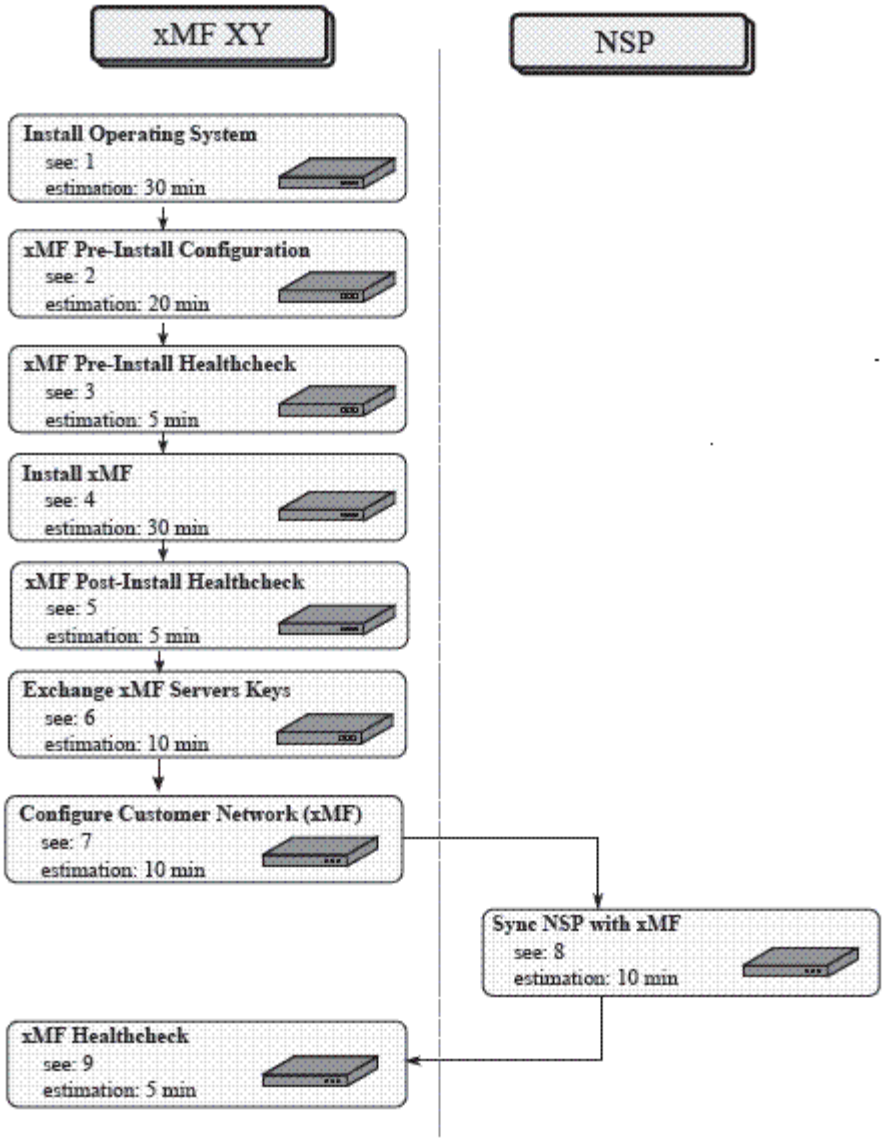
5. Login as `root` user on NSP Server (In case of One box configuration) or Weblogic Primary Box (In case of Four box configuration) and execute the following command

```
# service nspservice start
```

3 xMF Disaster Recovery Procedures

3.1 TPD5 xMF Server Disaster Recovery T1100, T1200, G5 , G6 and Gen8

This flowchart depicts the sequence of procedures that must be executed to disaster recovery server.

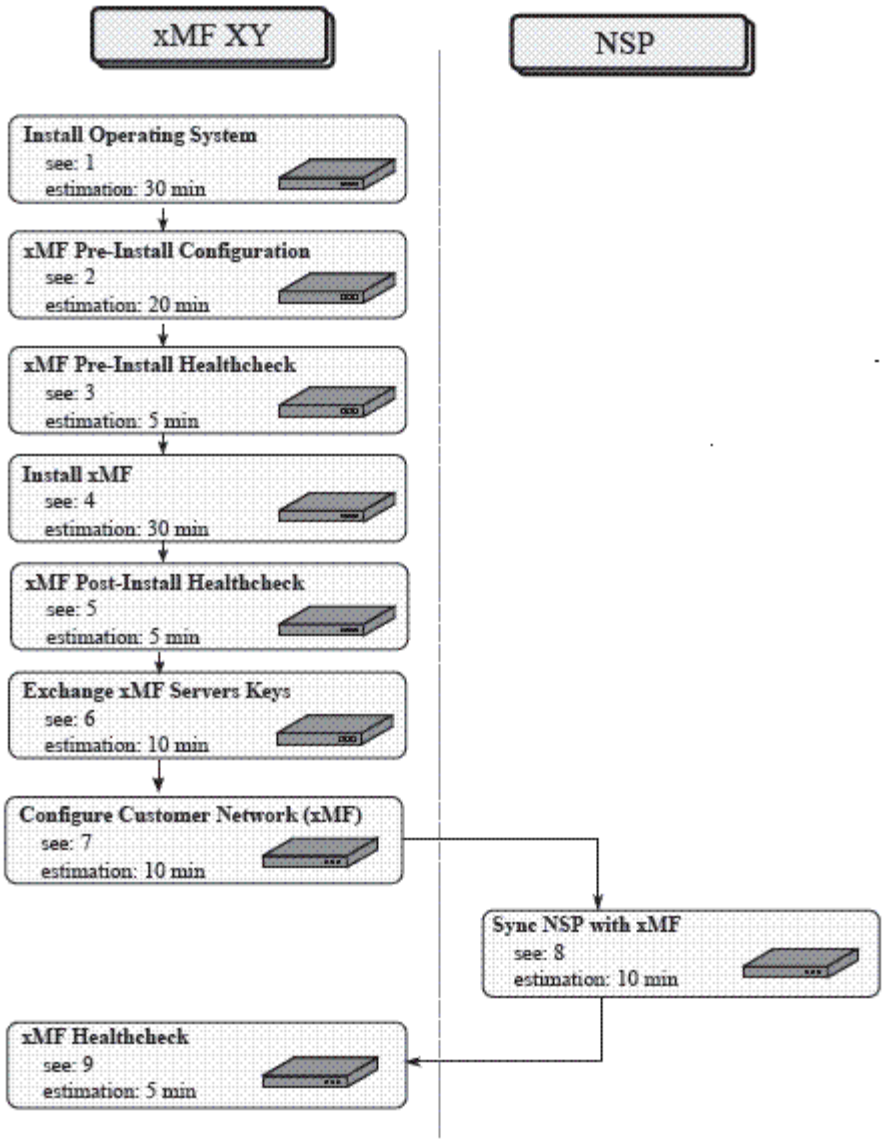


1. Refer to Install Operating System on xMF G5 Rackmount Servers or Install Operating System on xMF G6 Rackmount Servers or Install Operating System on T1200 Server or Install Operating System on T1100 Server or Install Operating System on Gen8 Rackmount Servers
2. Refer to xMF Pre-Install Configuration
3. Refer to xMF Pre-Install Healthcheck.
4. Refer to Install xMF.
5. Refer to xMF Post-Install Healthcheck.
6. Refer to Exchange xMF Servers Keys
7. Refer to TPD 5 Customer Network Configuration T1100, T1200, G5 G6 and Gen8

8. Refer to Sync NSP with xMF
9. Refer to xMF Healthcheck

3.2 TPD3 IMF 1A Server Disaster Recovery Overview for T1100

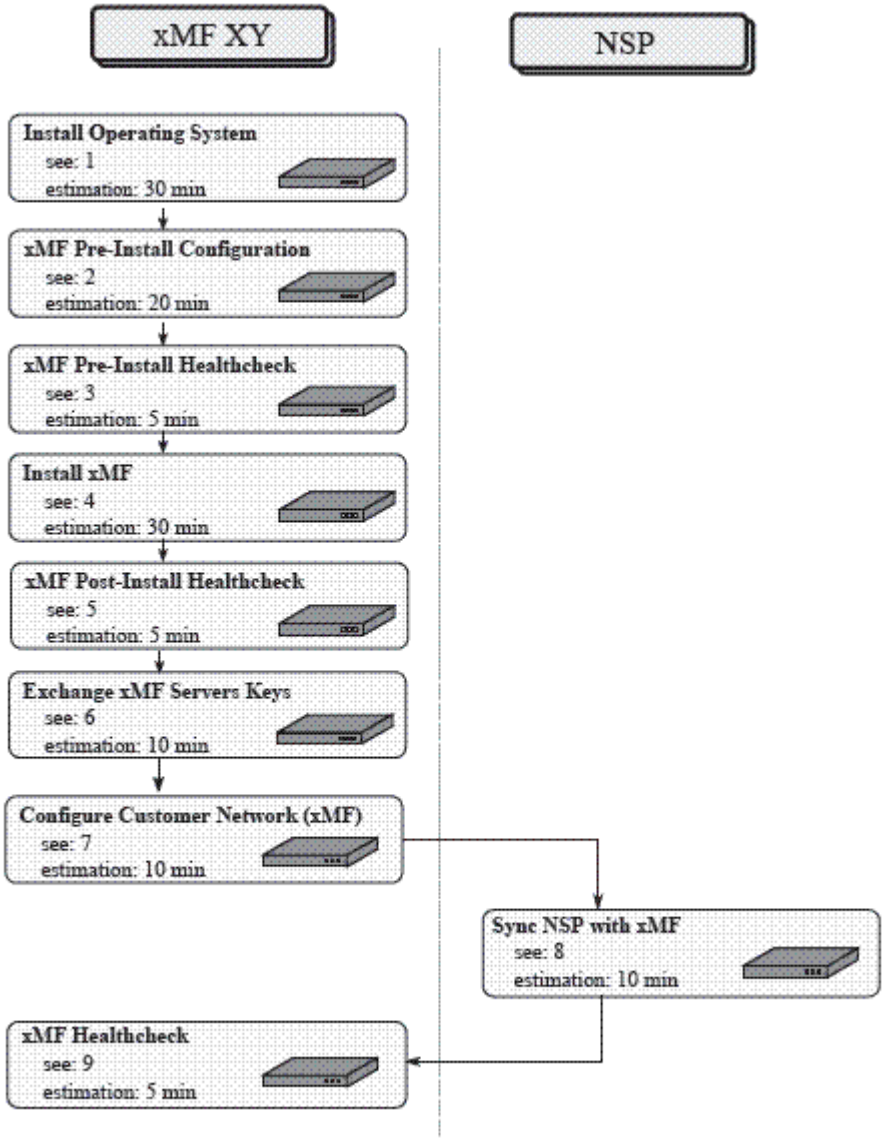
This flowchart depicts the sequence of procedures that must be executed to disaster recovery server.



1. Refer to Install Operating System on T1100 Server.
2. Refer to xMF Pre-Install Configuration.
3. Refer to xMF Pre-Install Healthcheck.
4. Refer to Install xMF.
5. Refer to xMF Post-Install Healthcheck.
6. Refer to Exchange xMF Servers Keys
7. Refer to TPD 3 Customer Network Configuration
8. Refer to Sync NSP with xMF
9. Refer to xMF Healthcheck

3.3 TPD3 IMF non-1A Server Disaster Recovery Overview for T1100

This flowchart depicts the sequence of procedures that must be executed to disaster recovery server.



1. Refer to Install Operating System on T1100 Server.
2. Refer to xMF Pre-Install Configuration
3. Refer to xMF Pre-Install Healthcheck.
4. Refer to Install xMF.
5. Refer to xMF Post-Install Healthcheck.
6. Refer to Exchange xMF Servers Keys
7. Refer to TPD3 Customer Network Configuration for non-1A on T1100
8. Refer to Sync NSP with xMF
9. Refer to xMF Healthcheck

3.4 xMF Pre-Install Configuration

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

3.4.1 Verify Pre-Installation Requirements

This procedure verifies that all pre-installation requirements have been met.

1. Verify that all required media and access capabilities are available

The following items are required prior to installing the xMF application:

- Make sure that you have the appropriate xMF DVD/CD or ISO file.
- Capability to log in to a server, such as a PC with a null modem cable to connect to the serial port

2. Remote control

Connect to the server.

- For T1000, use the MRV to remote control.
- For T1100, use the OOBM to remote control.
- For T1200, use the RMM to remote control.
- For HP, use iLO to remote control.

Remark: if you don't have DVD/CD and that your remote control doesn't provide you "Virtual Media" feature, then refer to Temporary xMF customer IP assignment to configure network acces and copy ISO file in /var/TKLC/upgrade directory.

3.4.2 Configure xMF

This procedure describes how to configure the xMF servers prior to installing the xMF application.
Note: This procedure must be executed on all of the IMF and PMF servers.

1. Log in and change the current hostname to the hostname provided by the customer

Note: The hostname must be changed from the default `localhost.localdomain` to desired hostname.

a) Log in as `root` on the xMF server.
b) Enter the **platcfg** menu. As `root`, run:

```
# su - platcfg
```

c) Select **Server Configuration** ⊙
Hostname. d) Click **Edit**.
e) Change the hostname and select **Exit**. For example, `malibu-1a`.

Note: In the field, there may be additional text that is hidden to the left of the visible text. It is recommended that you clear the field before typing the new hostname.

2. Change the current designation and function

Note: The designation and function are case sensitive and **must** be capitalized; otherwise, the software functionality will not work properly and will result in the need to reinstall the application.

a) Select **Server Configuration ⊙ Designation/Function**.
b) Select **Edit**.
c) Change the designation and function.

- For a PMF/IMF subsystem:

  In the **Function** field, enter `PMF` or `IMF`. In the **Designation** field, enter the designation in the following format: `1A` for the first server, `1B` for the second, and so on.

- For a standalone PMF:

In the **Function** field, enter `PMF`. In the **Designation** field, enter the `0A` for the server.
d) Select **Exit**.

3.4.3 Disable Hyper-threading on G6 Servers

This procedure describes how to disable Hyper-threading on a G6 server.

Disable Hyper-threading (only PMF)

Note: This step is applicable only for PMF.

a) Reboot the server.
b) As the computer boots, press **F9** to access the BIOS setup utility and press **Enter**. c) Select **System Options** and press **Enter**.
d) Select **Processor Options** and press **Enter**.

e) Select **Intel Hyper threading Options** and press **Enter**. f) Select **Disable** and press **Enter**.
g) Press **Esc** to exit the utility.
h) Press **F10** to confirm the exit from the utility.

3.5 xMF Pre-Install Healthcheck

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

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

```
# syscheck
```

3. Review the `fail_log` file (`/var/TKLC/log/syscheck/fail_log`) for any errors.
   Example ouput for a healthy system:

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

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

3.6 Install xMF

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

Before you perform this procedure, make sure that you have the appropriate xMF DVD/CD or ISO file available.

1. **Log in and insert the DVD/CD or copy the ISO file to the server**
   a) Open a terminal window and log in as `root` on the server that you are want to install the xMF application.
   b) Insert the xMF DVD/CD or mount the ISO file to the server.
2. **Validate the installation media**
   a) Enter the **platcfg** menu. As `root`, run:
   ```
   # su - platcfg
   ```
   b) Select **Maintenance ⊙ Upgrade ⊙ Validate Media**. c) Select the desired upgrade media and press **Enter**.
   The validation process must complete without errors. You should receive the following message: CDROM is Valid
   If any errors are reported during this validation process, then **DO NOT USE** this media to install the application.
   d) Exit the **platcfg** menu.
3. **Install the application**
   a) Enter the **platcfg** menu. As `root`, run:
   ```
   # su - platcfg
   ```
   b) Select **Maintenance ⊙ Upgrade ⊙ Initiate Upgrade**. c) Select the desired upgrade media and press **Enter**.
   Informational messages appear on the terminal screen as the upgrade proceeds. When the installation is complete, the server reboots and displays the login prompt.
   You can check the TPD upgrade log file (`/var/TKLC/log/upgrade/upgrade.log`) for any error; but the status of the server will be checked when you run the healthcheck script after you configure the switches.

3.7 xMF Post-Install Healthcheck

This procedure describes how to run the healthcheck script on xMF servers after the xMF application has been installed.

The script gathers the healthcheck information from the server on which the script was run. The output consists of a list of checks and results.

1. Log in as `cfguser` on the server that you want to check.
2. Run the automatic healthcheck script.
   ```
   $ analyze_server.sh -p
   ```
3. Analyze the output of the script for errors. Issues reported by this script must be resolved before any further usage of this server.

Example output for a healthy system:

```
08:33:00: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
08:33:00: date: 02-07-11, hostname: PMF0701-0A
08:33:00: TPD VERSION: 4.2.2-70.79.0
08:33:00: XMF VERSION: [ 70.1.0-17.1.0 ]
08:33:00: ------------------------------------------------
08:33:00: Checking disk free space
08:33:00:       No disk space issues found
08:33:00: Checking syscheck - this can take a while
08:33:03:       No errors in syscheck modules
08:33:03: Checking statefiles
08:33:03:       Statefiles do not exist
08:33:03: Checking runlevel
08:33:03:       Runlevel is OK (N 4)
08:33:03: Checking upgrade log
08:33:03:       Install logs are free of errors
08:33:03: Analyzing IDB state
08:33:03:       IDB in START state
08:33:03: Checking IDB database
08:33:04:       iaudit has not found any errors
08:33:04: Analyzing processes
08:33:04:       Processes analysis done
08:33:04: All tests passed. Good job!
08:33:04: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
```

Example output for a system with errors:

```
08:18:31: >>> Error: Syscheck analyzes contains alarms
One or more module in class "hardware" FAILED
08:18:32: >>> Suggestion: Check /var/TKLC/log/syscheck/fail_log at 1297084711
for more information
...
08:18:35: >>> Error: 1 test(s) failed!
08:18:35: ENDING HEALTHCHECK PROCEDURE WITH CODE 2
```

3.8 Exchange xMF Servers Keys

This procedure describes how to exchange the keys between xMF servers that allow automatic scripts to log in between servers without providing a password.

This procedure is performed after all of the xMF servers in the subsystem are installed.

Note: This procedure conserns on all kind of setup (subsystem and standalone).

1. **Run the exchange script**

   a) Log in as `cfguser` on the XMF-1A server.

   b) Run the `exchange_keys.sh` script; use the yellow network interfaces of all the servers in the frame as parameters. As `cfguser`, run:

   ```
   $ exchange_keys.sh yellow-1a yellow-1b ...
   ```

   At the start, the script prompts you for the cfguser password one time.

   Note: If asked for the RSA key during the execution, press **Enter** to confirm the question (**Yes** is the default value).

   This script first exchanges the keys and then verifies whether the exchange was successful. The period of time that the verification process takes varies depending on the system size; for larger subsystems, the time will be longer.

2. **Verify that the keys were successfully exchanged**

   a) Analyze the output of the script to determine whether the keys are successfully exchanged.

   Example output of a successful exchange for a frame with three IMF servers:

   ```
   === OK ===
   ssh keys were successfully exchanged between interfaces:
   ```

```
yellow-1a yellow-1b yellow-1c
```

Example output of a failed exchange (key exchange is not completed for all of the given interfaces)
for a frame with three IMF servers:

```
=== FAILED ===
there were found some connections which still requires password:
yellow-1c --> yellow-1a
yellow-1c --> yellow-1b
```

3.9 TPD 3 Customer Network Configuration for 1A on T1100

This procedure configures the CUST network on 1A (eventually on 0A) server. It is applicable on Tekserver 1 (T1000), Tekserver 2 (T1100) during disaster recovery

1. Log in and change the current hostname to the hostname provided by the customer

a) Login to server as root
b) Enter the **platcfg** menu. As `root`, run:

```
# su - platcfg
```

2. Set timezone

a) Select **Server Configuration ⊙ Time Zone**
b) Select appropriate time zone and confirm with **OK**

3. Configure CUST network

a) Select **Network Configuration ⊙ Configure Subnets**
b) Edit the **cust** network IP address of the frame and its net mask.

4. Edit existing default route

Note: There should be only one default route after default route configuration is finished.

a) Select **Network Configuration ⊙ Routing**
b) In **Edit default Route** menu choose proper network interface and edit the Gateway IP address. Then confirm. Possible interfaces:

- eth81.200 for Tekserver 1
- eth91.200 for Tekserver 2
- eth01.200 for Tekserver 3
- bond0.200 if `REDUNDANT WAN` is enabled

6. Configure NTP server

Note: For better time synchronization between mated sites servers should use the mated sites 1A (as ntppeer1) and 1B (as ntppeer2). All sites MUST sync from the same ntp source, ie: IP for ntpserver1 should be the same for each site.

You may receive the error message: `Could not set NTP servers! Failed to restart NTP!` You can ignore this message.Any time you change the NTP server on 1A, the ntpd process on the remaining servers needs to be restarted. While performing Customer Network Configuration you will be rebooting those servers later, so that will restart ntpd.

a) Select **Network Configuration ⊙ NTP**
b) Enter IP for NTP server on **ntpserver1** line.
c) Enter IP for the mated sites 1A server if applicable into **ntppeerA**. d) Enter IP for the mated sites 1B server if applicable into **ntppeerB**. e) Confirm and leave the platcfg utility
f) Move to directory:

```
# cd /var/yp
```

g) Update the yp maps

```
# make all
```

Output:

```
Updating hosts.byname...
Pushing hosts.byname map to blue-1b ... Updating hosts.byaddr...
Pushing hosts.byaddr map to blue-1b ...
```

7. Configure the NSP application server's IP address.

a) Run setAppServer script

```
# /usr/TKLC/TKLCmf/bin/setAppServer
```

```
Please enter an IP address for appserver:
```

b) Enter IP address of the weblogic primary server

Output should be similar to below(if there is only "Does the system have a 2nd Application Server (y or n) ? " it is correct too):

```
XX.XX.XX.XX         appserver

Old appserver entry not found.  Adding
RCS_VERSION=1.X
Updating hosts.byname... Updating hosts.byaddr...
Does the system have a 2nd Application Server (y or n) ?
```

C) For set the ip of the weblogic secondary server answer **y** otherwise **n.** If you do not want to set weblogic secondary server answer **n:**

```
#
```

If you want to set weblogic secondary server answer **y**:

```
Please enter an IP address for appserver2:
```

Enter IP address of the weblogic secondary server

```
Updating hosts.byname...
Pushing hosts.byname map to blue-1b ...
Updating hosts.byaddr...
Pushing hosts.byaddr map to blue-1b ...
#
```

8. Delete state file

Note: remove the mrv related state file from `/usr/TKLC/plat/etc/statefiles.d` directory.

a) As root run:

```
# rm/usr/TKLC/plat/etc/statefiles.d/NCSubnetConfig.mrv.statefile
```

9. Reboot the server

Note: The reboot may take up to 15 minutes while the switches are being updated.

10. Configure cust network on other (non-1A) server if applicable

Note: As root user run the following command to set up the customer network on each non-1A server of every frame. The following command should run first on all non-1A servers in the first frame before running it on the servers of other frame.

Note: If the current network configurations of the non-1A servers are different than 1A server running the below mentioned command on the non-1A server may cause the server to reboot to set the new network information. Only run during a maintenance window.

a) Restart NIS:

```
# service TKLCplnis start
```

3.10 TPD3 Customer Network Configuration for non-1A on T1100

This procedure configures the CUST network on non-1A servers. It is applicable on Tekserver 1 (T1000), Tekserver 2 (T1100) during disaster recovery

1. Log in and change the current hostname to the hostname provided by the customer

a) Login to server as root
b) Enter the **platcfg** menu. As `root`, run:

```
# su - platcfg
```

2. Set timezone

a) Select **Server Configuration ⊙ Time Zone**
b) Select appropriate time zone and confirm with **OK**

3. Edit existing default route

Note: There should be only one default route after default route configuration is finished.

a) Select **Network Configuration ⊙ Routing**
b) In **Edit default Route** menu choose proper network interface and edit the Gateway IP address.

Then confirm. Possible interfaces:

- eth81.200 for Tekserver 1
- eth91.200 for Tekserver 2
- eth01.200 for Tekserver 3
- bond0.200 if `REDUNDANT WAN` is enabled

4. Reboot the server

3.11 TPD 5 Customer Network Configuration T1100, T1200, G5 G6 and Gen8

This procedure describes how to configure the customer network.

Before you perform this procedure, make sure you have read and are familiar with the xMF Bulkconfig File Description

1. Create the bulkconfig file

a) Open a terminal window and log in as `root` on the xMF server.
b) Create the bulkconfig file.
c) Verify the file is in the proper directory.
As `root`, run:

```
# ls /var/TKLC/upgrade/platform.csv
```

2. Run the bulkconfig script

a) Run bulkconfig script. As `root`, run:

```
# bulkConf.pl
```

Example of correct output:

```
Name: imf-1a
        Func: IMF
        Desig: 1A
        Cust: bond0.200
        HostIp: 192.168.253.5
        Mask: 255.255.255.224
        Route: 192.168.253.1
        Updating hostname to imf-1a.
        LiveIP: 192.168.253.5...
NTP: ntpserver1
        Ip: 10.250.32.10
        Updating ntpserver1...
NTP: ntpserver2
        Ip: 10.250.32.11
        Updating ntpserver2...
NTP: ntpserver3
        Ip: 10.250.32.12
        Updating ntpserver3...
NTP: ntppeerA
        Ip: 10.250.32.13
        Updating ntppeerA...
NTP: ntppeerB
        Ip: 10.250.32.14
        Updating ntppeerB...
APP: appserver
        Ip: 10.10.10.10
        Adding new appserver...
APP: appserver2
        Ip: 10.10.10.11
        Adding new appserver...
TZ: Europe/Prague
        Updating Timezone America/New_York to Europe/Prague...
```

b) Verify there are no errors in the script output. If an error occurs in the output contact the Tekelec

Customer Care Center.

Example of ouput with errors:

```
01:22:17: Ntp settings is OK
01:22:17: Analyzing IDB state
01:22:17: >>> Error: IDB is not in started state (current state X)
01:22:17: >>> Suggestion: Verify system stability and use 'prod.start' to start
 the product
01:22:17: Checking IDB database
01:22:17:       iaudit has not found any errors
01:22:17: Analyzing processes
01:22:17:       Processes analysis done
01:22:17: Analysing database synchronization
01:22:18:       Database synchronization in healthy state
01:22:18: Checking weblogic server entry
```

```
01:22:18:       Appserver is present
01:22:18: Checking whether ssh dsa key was generated
01:22:18:       This test is not performed on standalone server
01:22:18: Checking whether ssh keys are exchanged among machines in frame - this can
take a while
01:22:18:       Standalone server - no need to have exchanged keys
01:22:18: Checking A-Node server
01:22:18: >>> Warning: A-Node wasn't defined yet
01:22:18: >>> Suggestion: perform procedure for site and subsystem configuration
 or install A-Node server
01:22:18: Checking version of the nsp
01:22:18: >>> Error: nsp wasn't defined yet
01:22:18: >>> Suggestion: perform procedure for site and subsystem configuration
01:22:18: >>> Error: 3 test(s) failed!
01:22:18: ENDING HEALTHCHECK PROCEDURE WITH CODE 3
```

c) Reboot the server.

3.12 Sync NSP with xMF

1. Discover xMF Applications

a) From supported browser login to the NSP Application GUI as privileged user

b) Go to the Centralized Configuration

c) Navigate to **Equipment Registry Perspective** in left tree

panel. d) Navigate to the subsystem.

e) Select the XMF subsystem to synchronize by clicking on **XMF** under the correct Site

name. f) This will list the subsystem in the table

g) Click the **Synchronize** action in the table row for the XMF subsystem.

Note: This action includes both Application synchronization and Network Element synchronization

2. Apply Changes xMF

a) To Apply Changes for each subsystem go to **Acquisition ⊙ Sites ⊙ XMF.**

b) Right click on subsystem and click on **Apply Changes** option on menu.

Note: If there were some errors remove link sets from the **Links View**, then re-add it again and do the **Apply changes** (it could be necessary to remove the links from the **Monitoring Group** before removing. In that case it should be added to the **Monitoring Group** after **synchronization**)

3. Test the VIP function.

a) After sync from NSP, the VIP will be available to access the active master server in the site. In order to verify the VIP setup please login to any server in the subsystem and execute the **`iFoStat`** command:

```
$ iFoStat
```

Example of correct output:

```
query 10.236.2.79 for failover status
+---------+-------+-----+-----------+----------+------+----------------------+
| name    | state | loc | role      | mGroup   | assg | HbTime               |
+---------+-------+-----+-----------+----------+------+----------------------+
| tek3-1a | IS    | 1A  | ActMaster | sde_m2pa |    8 | 2009-06-19 23:14:08 |
```

```
| tek3-1b | IS    | 1B  | StbMaster | sde_stc  |    6 | 2009-06-19 23:14:06 |
| tek3-1c | IS    | 1C  | Slave     |          |    0 | 2009-06-19 23:14:06 |
+---------+-------+-----+-----------+----------+------+---------------------+
```

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

3.13 xMF Healthcheck

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

The script gathers the healthcheck information from each server in the xMF subsystem or from standalone server. The script should be run from only on one server of the XMF subsystem (the 1A server is prefered) or on stand-alone. The output consists of a list of checks and results, and, if applicable, suggested solutions.

1. Open a terminal window and log in as `cfguser` on any server in the xMF subsystem or standalone server.
2. Run the automatic healthcheck script.

   ```
   $ analyze_subsystem.sh
   ```

3. Analyze the output of the script for errors. Issues reported by this script must be resolved before any further usage of this server. Verify no errors are present.

   If the error occurs, contact the Tekelec Customer Care Center.

   Note: For a standalone, there will be only one server in the ouput.

   Example output for a healthy subsystem:

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

11:28:59: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
11:28:59: date: 02-07-11, hostname: IMF0502-1A
11:28:59: TPD VERSION: 3.3.8-63.25.0
11:28:59: XMF VERSION: [ 60.6.7-2.1.0 ]
11:28:59: ------------------------------------------------
11:28:59: Checking disk free space
11:28:59:       No disk space issues found
...
11:29:08: Checking whether ssh keys are exchanged among machines in frame - this
 can take a while
11:29:08:       3 mates found: yellow-1B yellow-1C yellow-1D
11:29:26:       Connection to all mates without password was successful
11:29:26: Checking A-Node server
11:29:29:       Connection to A-Node 10.240.9.4 was successful
11:29:29:       A-Node version is: 60.6.7-2.1.0
11:29:29: Checking version of the nsp
11:29:32:       Connection to nsp 10.240.9.3 was successful
11:29:32:       nsp version is: 6.6.4-7.1.0
11:29:32:       nsp was installed on: 2011-01-13 05:09:26 (25 days 6 hours ago)
11:29:32: All tests passed. Good job!
11:29:32: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0502-1A

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

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

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

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

Example output for a subsystem with errors:

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

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

4 IXP Disaster Recovery Procedures

4.1 IXP 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:

- IXP xDR Storage Server
- IXP PDU Storage Server
- IXP Base Server
- Export Server (Low-Cost Export Server will be installed automatically if no external storage will be detected)

The procedure is applicable to the following hardware types:

- HP G5 DL360
- HP G6 DL360
- HP G1 BL460
- HP G5 BL460
- HP G6 BL460

This disaster recovery procedure is also part of the disaster recovery procedures of the following applications:

- Report Server - as disaster recovery of IXP xDR Storage server
- Post Process Service (PPS) - as disaster recovery of IXP Base server

Note: The Low-Cost Export Server has no external storage like regular Export Server (ES) has. All exported files are stored on internal disk only. As the server is reinstalled during the disaster recovery process all exported data on internal disk will be lost. There is no space to backup those data.

Note: During the disaster recovery procedure of IXP xDR Storage Server you must install the same version of the Oracle database as the current one. If there is Oracle 10g installed then install Oracle
10g during the disaster recovery process. If Oracle 11g is currently installed then install Oracle 11g during disaster recovery. In any other case the disaster recovery procedure will fail. Check the Oracle version on the IXP xDR Storage Server as `root` with the following command:

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

Note: It's 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

Note: If PPS is installed on any IXP server, backups of XMLs needs to be taken from PPS server before executing the recovery procedure on IXP server.
Login to PPS server and execute below command

```
root#   scp -r /var/TKLC/ixp/ppsxmls/ root@<IP>:/var/TKLC/
```

where <IP> is the IP address of the server on which the backup will be saved.

Skipping this step will result in KPI loss after system is recovered.

The following references depicts the sequence of procedures that must be executed to recover

the specific IXP server type and associated server functions.

4.1.1 IXP xDR Storage server disaster recovery procedure

Follow the references below in a sequential order to recover the IXP xDR Storage server.

1. Refer to Stop IXP Service
2. Refer to Disintegrate Server with the IXP Subsystem
3. Refer to Stop Oracle Service
4. Refer to Backup Oracle Control and Configuration Files (Oracle 10g only)
5. Install the operating system.
   - For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
   - For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
   - For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
   - For C-class blade follow IPM Blade Servers Using PM&C Application
6. Refer to Remount IXP LUN (C-class blades only)
7. Refer to IXP Pre-Install Configuration
8. Refer to Install Oracle Database
9. Refer to Install IXP
10. Refer to IXP Post-Install Healthcheck
11. Refer to Integrate Server with the IXP Subsystem
12. Refer to Restore xDR Builders
13. Refer to xDR Builders Licensing
14. Refer to Remove Backup Directory
15. Refer to Remount Export Directories

4.1.2 IXP PDU Storage server and IXP ES server disaster recovery procedure.

Follow the references below in a sequential order to recover the IXP PDU Storage server or IXP Export server.

1. Refer to Stop IXP Service
2. Refer to Disintegrate Server with the IXP Subsystem
3. Install the operating system.
   - For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
   - For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
   - For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
   - For C-class blade follow IPM Blade Servers Using PM&C Application
4. Refer to Remount IXP LUN (C-class blades only)
5. Refer to IXP Pre-Install Configuration
6. Refer to Install IXP
7. Refer to IXP Post-Install Healthcheck
8. Refer to Integrate Server with the IXP Subsystem
9. Refer to Restore xDR Builders
10. Refer to xDR Builders Licensing
11. Refer to 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.

1. Refer to Stop IXP Service
2. Refer to Disintegrate Server with the IXP Subsystem

3. Install the operating system.
   - For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
   - For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
   - For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
   - For C-class blade follow IPM Blade Servers Using PM&C Application
4. Refer to IXP Pre-Install Configuration
5. Refer to Install IXP
6. Refer to IXP Post-Install Healthcheck
7. Refer to Integrate Server with the IXP Subsystem
8. Refer to Restore xDR Builders
9. Refer to xDR Builders Licensing
10. Refer to Remount Export Directories

4.2 Stop IXP Service

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

Stop IXP service

a) Open a terminal window and log in as `root` on the IXP server.

As `root` run:

```
# 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. Disintegrate server with the IXP subsystem.

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 Stop Oracle Service

This procedure describes how to stop Oracle service on the IXP server. This procedure is applicable to IXP xDR Storage server only.

Stop Oracle service

a) Open a terminal window and log in as `root` run on the IXP server.

As `root` run:

```
# service TKLCoracledb stop
```

b) Wait until Oracle service stops:

```
# ps -ef | grep ora | grep -v grep
```

4.5 Backup Oracle Control and Configuration Files (Oracle 10g only)

This procedure describes how to Oracle control and configuration files. This procedure is applicable to IXP xDR Storage server only. This procedure is applicable to Oracle 10g release only.

Backup Oracle control and configuration files

a) Open a terminal window and log in as `root` on the IXP server.

b) Backup Oracle control and configuration files. As `root` run:

```
# misc_backup_oracle.sh --backup
```

4.6 Remount IXP LUN (C-class blades only)

This procedure describes how to remount the IXP LUN. The procedure is applicable to xDR Storage Server, PDU Storage Server and Export Server only.

1. Retrieve volume names and LUN numbers from SAN configuration file

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

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

a) 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

3. **Remount LUN**

a) Copy the IXP ISO file to the server.

b) Open a terminal window and log in as `root` to the IXP server and mount the ISO. As `root` run:

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

where *iso_fath* is the path to the IXP ISO file including the ISO filename.

c) Repeat the following command for each LUN you need to mount. As `root` run:

```
# /mnt/upgrade/ixp/remapVolume name volume_name lun lun_number
```

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.

d) 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. **Umount the IXP ISO**

Note: Execute an IPM on the failed server. Follow section: TODO add LINK

a) As `root` run:

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

4.7 IXP Pre-Install Configuration

This procedure describes how to configure IXP prior to installing the IXP application.

Before you perform this procedure, make sure you have read and are familiar with the IXP Bulkconfig File Description

Note: When creating a `bulkconfig` file on a server in the IXP subsystem, if such a file has already been created on a different server, then reuse that `bulkconfig` file. The content of the

`bulkconfig` file is the same for all servers (except for the optional EFS) in the IXP subsystem.

1. **Verify the server healthcheck.**

   a) Run syscheck. Log in as `root` on the server that you want to install the application. As `root` run:

```
# syscheck
```

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

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

Running modules in class proc...
                                  OK

Running modules in class system...
                                  OK

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

   Resolve each error before you continue with the procedure.

   Note: Errors of NTP in syscheck can be ignored at this time, as NTP server is not configured b) If the server has an external disk storage attached verify the disks state.

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

```
# hpacucli ctrl all show
```

   Example output:

```
[root@ixp0301-1a ~]# hpacucli ctrl all show
Smart Array 6400 in Slot 2                (sn: P5782AT9SX5017)
Smart Array P400i in Slot 0 (Embedded)    (sn: PH95MP6416     )
```

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

```
# hpacucli ctrl slot=slot_number pd all show
```

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

```
[root@ixp0301-1a ~]# hpacucli ctrl slot=2 pd all show

Smart Array 6400 in Slot 2
   array A
      physicaldrive 1:0   (port 1:id 0 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:1   (port 1:id 1 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:2   (port 1:id 2 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:3   (port 1:id 3 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:4   (port 1:id 4 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:5   (port 1:id 5 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:8   (port 1:id 8 , Parallel SCSI, 300 GB, OK)

   array B
      physicaldrive 2:0   (port 2:id 0 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:1   (port 2:id 1 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:2   (port 2:id 2 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:3   (port 2:id 3 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:4   (port 2:id 4 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:5   (port 2:id 5 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:8   (port 2:id 8 , Parallel SCSI, 300 GB, OK)
```

2. Create the bulkconfig file

a) As a `root` user.
b) Create the `/root/bulkconfig` file.

3. Configure the server hostname

a) Enter the **platcfg** menu.

As `root`, run:

```
# su - platcfg
```

b) Select **Server Configuration ⊙ Hostname**
. c) Click **Edit**.
d) Enter the server hostname in the standard format: `ixp`*`NNNN-MA`* .
where:

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

Note: Each subsystem must have the same *NNNN* designation, while the individual server is identified by the *MA* designation (for example, `1A`).

e) Exit the **platcfg** menu.

4.8 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 DVD/CD or ISO file available.
- Verify the `/root/bulkconfig` file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.
- In case of c-class blades SAN Configuration must be done properly before starting Oracle Installation
.
- This procedure must be run via iLO.

WORKAROUND PR196740: If the server changed its function or different version of Oracle was previously installed manually, clean up first ~1000MB of each partition using dd command before Oracle installation.

1. Log in and either insert the DVD/CD or distribute the ISO file

a) Log in as `root` on the server where you want to install the Oracle database. b) Distribute the media:

- On the rackmout server insert the Oracle DVD/CD or mount the Oracle ISO file via iLO (see How to mount the ISO file via iLO).
- On the c-class blade server download the ISO from the PM&C ISO repository. ISOs are available on the PM&C server under the `/var/TKLC/smac/image` directory. Store the ISO file to `/var/TKLC/upgrade` directory. If the ISO is not present in PM&C ISO

repository add the ISO file using the procedure Adding ISO Images to the PM&C Image Repository

2. **Validate the installation media**

   a) Enter the **platcfg** menu. As `root`, run:

   ```
   # su - platcfg
   ```

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

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

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

   d) Exit the **platcfg** menu.

3. **Mount the media**

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

   - For a DVD/CD (rackmount server), run:

     ```
     # mount /dev/cdrom /media
     ```

   - For an ISO mounted via iLO (rackmout server), run:

     ```
     # getCDROMmedia
     ```

     to check which CDROM device has been added to the `/dev/` directory. Example output:

     ```
     # getCDROMmedia
     HP Virtual DVD-ROM:scd0
     ```

     This example output denotes virtual CD-ROM device `/dev/scd0`. Then mount this device to `/media` directory.

     ```
     # mount -o loop virtual_cdrom_device /media
     ```

     where *virtual_cdrom_device* is the path to virtual CD-ROM device received in a previous step.

   - For an ISO file (c-class server), run:

     ```
     # mount -o loop /var/TKLC/upgrade/iso_file /media
     ```

     where *iso_file* is the ISO filename.

4. **Install Oracle**

   As `root`, run:

   ```
   # /media/install_oracle.sh
   ```

   Note: When installing Oracle 11g you will be prompted by the following:

   ```
   You are about to install Oracle 11G and ASM. Are you sure you want to continue
   (yes/no)
   ```

Type `yes` to confirm. Press `<enter>` to continue.

When the installation process is complete the server will automatically reboot.

5. **Remove the ISO file.**

   a) After reboot open a terminal window and log back in as `root`.

   b) If the ISO file was copied to the server, then remove this file to save disk space. As `root`, run:

```
# rm -f /var/TKLC/upgrade/iso_file
```

where *iso_file* is the ISO filename.

6. **Analyze the installation log**

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

   If there are any errors, contact the Tekelec Customer Care Center.

4.9 Install IXP

This procedure describes how to install the IXP application on the TPD platform.
Before you perform this procedure, make sure that you have the appropriate IXP DVD/CD or ISO file available.

Verify the `/root/bulkconfig` file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.

Note: Run this procedure via iLO.

1. **Log in and insert the IXP DVD/CD or distribute the ISO file**

   a) Open a terminal window and log in as `root` on the server you that you want to install the IXP application.
   b) Distribute the media:

   - On the rackmount server insert the IXP DVD/CD or mount the IXP ISO file via iLO (see How to mount the ISO file via iLO).
   - On the c-class blade server download the ISO from the PM&C ISO repository. ISOs are available on the PM&C server under the `/var/TKLC/smac/image` directory. Store the ISO file to `/var/TKLC/upgrade` directory.

2. **Validate the installation media**

   a) Enter the **platcfg** menu. As `root`, run:

   ```
   # su - platcfg
   ```

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

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

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

   d) Exit the **platcfg** menu.

3. **Install the application**

   a) Enter the **platcfg** menu. As `root`, run:

   ```
   # su - platfg
   ```

   b) Select **Maintenance ⊙ Upgrade ⊙ Initiate Upgrade**.
   When the installation process is complete, the server restarts automatically.
   c) If the ISO file was copied to the server, then remove this file to save disk space. As `root`, run:

```
# rm -f /var/TKLC/upgrade/iso_file
```

where *iso_file* is the absolute path of the ISO image, which includes the name of the image.

4. **Analyze the installation log**

Review the installation log (`/var/TKLC/log/upgrade/upgrade.log`) for any errors.

If there are any errors, contact the Tekelec Customer Care Center.

4.10 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. **Integrate recovered server with the IXP subsystem.**
   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.

4.11 IXP Post-Install Healthcheck

This procedure describes how to run the server healthcheck after the application has been installed on the server.

1. Log in on the server that you want to analyze.
2. As `cfguser`, run:

   ```
   $ analyze_server.sh -p
   ```

   The script gathers the healthcheck information from the server. A list of checks and associated results is generated. There might be steps that contain a suggested solution. Analyze the output of the script for any errors. Issues reported by this script must be resolved before any further use of this server.

   The following examples show the structure of the output, with various checks, values,

suggestions, and errors.

Example of overall output:

```
[cfguser@ixp8888-1a ~]$ analyze_server.sh
12:40:30: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
12:40:30: date: 08-22-11, hostname: ixp8888-1a
12:40:30: TPD VERSION: 4.2.4-70.90.0
12:40:30: IXP VERSION: [ 7.1.0-64.2.0 ]
12:40:30: XDR BUILDERS VERSION: [ 7.1.0-37.1.0 ]
12:40:30: ------------------------------------------------
12:40:31: Analyzing server record in /etc/hosts
12:40:31:       Server ixp8888-1a properly reflected in /etc/hosts file
12:40:31: Analyzing IDB state
12:40:31:       IDB in START state
12:40:31: Analyzing shared memory settings
12:40:31:       Shared memory set properly
.....
12:43:02: All tests passed!
12:43:02: ENDING HEALTHCHECK PROCEDURE WITH CODE 2
```

Example of a successful test:

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

Example of a failed test:

```
12:21:48: Analyzing IDB state
12:21:48: >>> Error: IDB is not in started state (current state X)
12:21:48: >>> Suggestion: Verify system stability and use 'prod.start' to start
 the product
```

After attempting the suggested resolution, if the test fails again, then contact Tekelec Customer Care Center.

4.12 Restore xDR Builders

This procedure describes the xDR builders installation handled from the IXP server. This procedure will download the xDR builders `*.rpm` from the NSP and install locally.

Note: 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.

Install xDR Builders package

a) Open a terminal window and log in to the IXP server as `cfguser`.

b) To install the builders, 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.

4.13 xDR Builders Licensing

This section describes how to generate and apply the xDR builders license key.

4.13.1 Use IXP Site Code to Generate xDR Builder License Key

This procedure describes how to use the valid `IxpSubsystemKey.data` file from the IXP subsystem to generate the xDR Builder license key.

Note: The `IxpSubsystemKey.data` file is generated on the IXP Active Master server after the IXP subsystem is configured or the server is added to the IXP subsystem.

1. **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.

2. **Send an email with a request to receive the license key file**

   Copy the `IxpSubsystemKey.data` file to a machine with an email access; then, send the file, along with a copy of the purchase order where the license part numbers are mentioned, to the following address: `cssg.product.license.request@tekelec.com`

4.13.2 Install xDR Builder License Key

This procedure describes how to install the xDR license key file on the IXP Active Master server.
Note: The xDR license key file (`IxpLicenseKey.data`) is attached to the response to the license request email.

1. **Transfer the license file to the IXP Active Master server**

   a) Open a terminal window and log in as cfguser on the IXP Active Master server.

   b) Copy the IxpLicenseKey.data file to the IXP Active Master server to /home/cfguser/

   directory.

2. **Activate license**

   As soon as the file has been detected and verified, the existing temporary license alarm(s), if any, is automatically cleared.

3. **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.

4.14 Remove Backup Directory

This procedure describes how to backup of the Oracle control and configuration files taken during the backup procedure for disaster recovery purpose.

Remove Backup Directory

a) Open a terminal window and log in to the IXP server as `root` .
b) As `root` run:

```
# rm –rf /opt/oracle/oradata/migration
```

4.15 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.

Remount export directories

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

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

c) DataFeed will mount exporting directories back by itself.

5 Export File Server Disaster Recovery Procedures

5.1 Export File Server Disaster Recovery Overview

This section describes how to execute a disaster recovery procedure of the Export File Server (EFS). The list of the references below depicts the sequence of procedures that must be executed in sequential order to recover the EFS server.

Export File Server (EFS) Disaster Recovery

1. Stop IXP Service. Refer to Stop IXP Service
2. Install the operating system. Refer to:
   - For rackmount HP G5 servers refer to Install Operating System on G5 Rackmount Servers
   - For rackmount HP G6 servers refer to Install Operating System on G6 Rackmount Servers
   - For HP C-Class blade servers refer to IPM Blade Servers Using PM&C Application
3. Remount IXP LUN. Execute only on C-Class blade servers. Refer to Remount IXP LUN (C-class blades only)
4. Execute pre-install configuration. Refer to EFS Pre-Install Configuration
5. Install EFS application. Refer to Install EFS
6. Execute EFS healthcheck. Refer to EFS Post-Install Healthcheck
7. Remount DataFeed export directories. Refer to Remount Export Directories
8. Adjust EFS network settings. Refer to Adjust EFS server
9. Integrate back EFS server with IXP subsystem. Refer to Reintegrate EFS with IXP subsystem

5.2 Stop IXP Service

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

Stop IXP service

a) Open a terminal window and log in as `root` on the IXP server.

As `root` run:

```
# service TKLCixp stop
```

5.3 Install Operating System on G5 Rackmount Servers

This procedure describes how to install the operating system on HP G5 rackmount servers.

1. Date and Time setup

a) Power on the server.

b) Power on disk arrays if they are connected.

c) Wait until the server will boot to the following message:

```
Press "F9" key for ROM-based Setup Utility
Press "F10" key for System Maintenance Menu
Press "F12" key for PXE boot
```

d) Press <F9> to enter **ROM-Based Setup Utility**
e) Navigate to **Date and time**
f) Set actual date end time
g) Press <ENTER>
h) Insert TPD CD into drive
i) Leave setup utility

2. Enter Installation Mode

a) Let system boot into TPD installation screen.
b) Enter installation parameters:

- If the external storage disk array is attached to server enter:

  For serial console:

  ```
  boot: TPDnoraid drives=cciss/c1d0 console=ttyS0
  ```

  For VGA/keyboar and iLO:

  ```
  boot: TPDnoraid drives=cciss/c1d0 console=tty0
  ```

- If the extarnal storage disk array is not attached to server enter:

  For serial console:

  ```
  boot: TPDnoraid console=ttyS0
  ```

  For VGA/keyboard and iLO:

  ```
  boot: TPDnoraid console=tty0
  ```

c) The installation process will display the progress of the system and packages installation.
d) At the end of installation the CD will be ejected from CD-ROM drive.
Remove the CD from tray and press <ENTER> to reboot the server.

5.4 Install Operating System on G6 Rackmount Servers

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

Before you perform this procedure, make sure that you have the appropriate TPD DVD/CD or ISO file available.

1. Power on and enter the BIOS

a) Power on the external disk arrays.
b) Power on the server.
Within a couple of seconds, the F9 Setup message appears in the bottom-right corner.
c) Press **F9**.
The message changes to F9 Pressed.

2. Set up the BIOS date and time

a) Select the **Main** menu and set the **System Date** and **System Time** values to Greenwich Mean Time (GMT).
b) Insert the TPD DVD/CD.

3. Set up the BIOS iLO

Note: The serial ports on HP DL360 and DL380 G6 rackmount servers need to be configured so that the serial port used by the BIOS and TPD are connected to the iLO Virtual Serial Port (VSP). This allows the remote administration of the servers without the need for external terminal servers. If this configuration has not been completed correctly and the server is rebooted, then the syscheck test (`syscheck -v hardware serial`) will fail.

a) Select **System Options ⊙ Serial Port Options**. b) Change the following settings:

- **Embedded Serial Port** to **COM2**
- **Virtual Serial Port** to **COM1**

c) Save the changes and exit the BIOS.
The system boots to the TPD installation screen.

4. Install the operating system

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

- For the serial console, enter:

```
boot: TPDnoraid console=ttyS0 diskconfig=HPG6,force
```

- For the iLO or VGA/keyboard, enter:

```
boot: TPDnoraid console=tty0 diskconfig=HPG6,force
```

5. Reboot the 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.

5.5 IPM Blade Servers Using PM&C Application

This procedure will provide the steps how to install TPD using image from PM&C image repository. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

1. PM&C GUI: Login

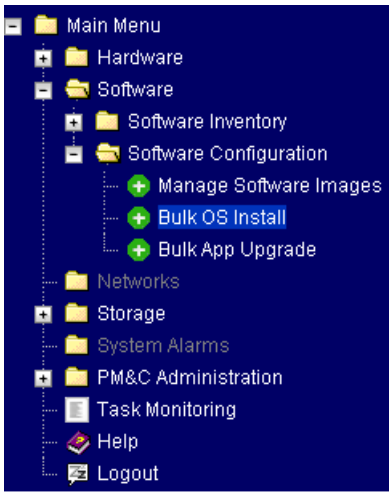
If needed, open web browser and enter:

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

Login as pmacadmin user.

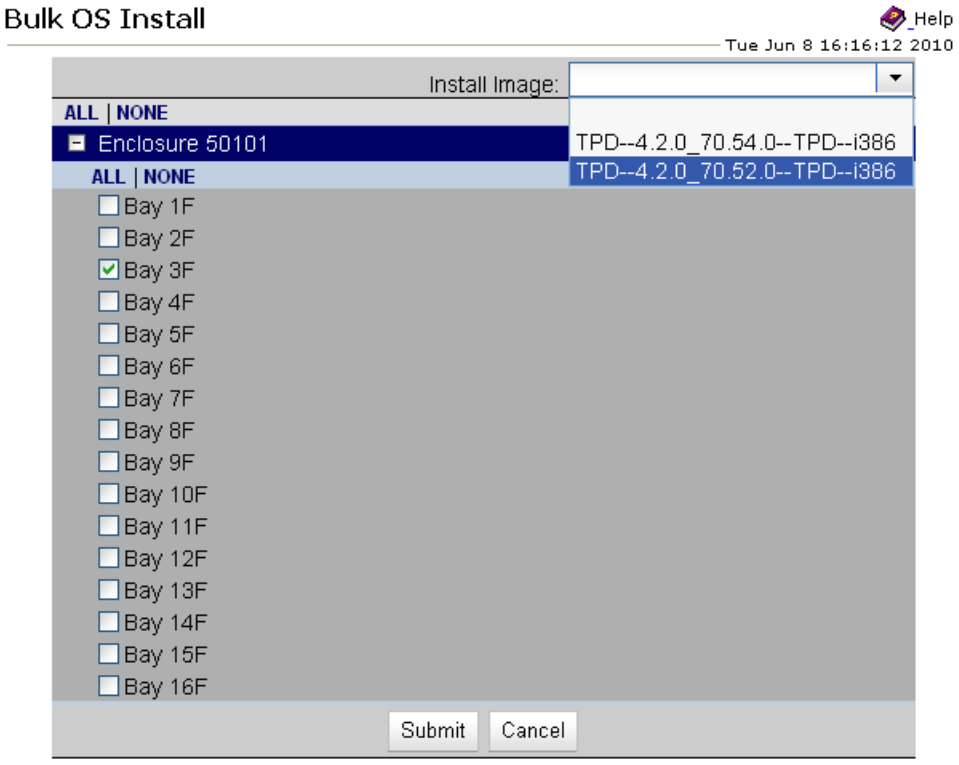
2. PM&C GUI: Navigate to Bulk OS install

Navigate to Software ➤Software Configuration ➤Bulk OS Install.



3. PM&C GUI: Initiate Bulk OS Install

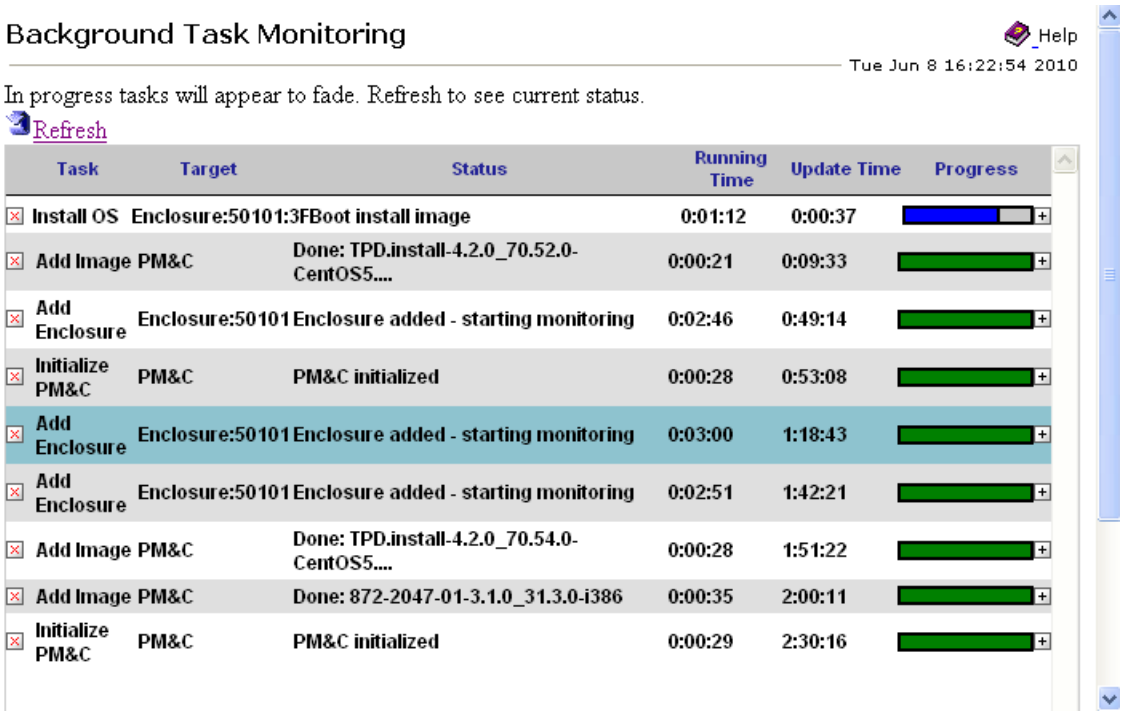
Expand the enclosure button. Select the TPD image you want to install. Select the blade that you want to install the image on, in a given enclosure. you may select multiple blades within each enclosure



Then press the **Submit** button and **Continue** button on `Confirm OS Install` popup. Then observe the `Done` message and press **Continue** button again.

4. PM&C GUI: Monitor the installation status

Navigate to **Task Monitoring** to check the installation status. Observe the blue bar of `Progress` - use refresh. Each blade is a separate task.



When the installation completes, the Progress bar turns green

5.6 Remount IXP LUN (C-class blades only)

This procedure describes how to remount the IXP LUN. The procedure is applicable to xDR Storage Server, PDU Storage Server and Export Server only.

1. **Retrieve volume names and LUN numbers from SAN configuration file**

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

2. **Remount LUN**

   a) Copy the IXP ISO file to the server.

   b) Open a terminal window and log in as `root` to the IXP server and mount the ISO. As `root` run:

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

   where *iso_fath* is the path to the IXP ISO file including the ISO filename.

   c) Repeat the following command for each LUN you need to mount. As `root` run:

   ```
   # /mnt/upgrade/ixp/remapVolume name volume_name lun lun_number
   ```

   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.

   d) After completion you have to see along with the other output:

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

3. **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]
```

4. Umount the IXP ISO

Note: Execute an IPM on the failed server. Follow section: TODO add LINK

a) As `root` run:

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

5.7 EFS Pre-Install Configuration

This procedure describes how to configure Export Filer Server (EFS) prior to installing the EFS application.

Before you perform this procedure, make sure you have read and are familiar with the *EFS Bulkconfig File Description*.

Note: For the EFS server, you must create a new and unique `bulkconfig` file. Do **not** copy and reuse the `bulkconfig` file that was created for the servers in the IXP subsystem.

1. Verify the server healthcheck.

a) Run syscheck. Log in as `root` on the server that you want to install the application. As `root` run:

```
# syscheck
```

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

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

Running modules in class proc...
                                  OK

Running modules in class system...
                                  OK

Running modules in class hardware...
                                  OK

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

Resolve each error before you continue with the procedure.

Note: Errors of NTP in syscheck can be ignored at this time, as NTP server is not configured b) If the server has an external disk storage attached verify the disks state.

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

```
# hpacucli ctrl all show
```

Example output:

```
[root@ixp0301-1a ~]# hpacucli ctrl all show
Smart Array 6400 in Slot 2                (sn: P5782AT9SX5017)
Smart Array P400i in Slot 0 (Embedded)    (sn: PH95MP6416     )
```

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

```
# hpacucli ctrl slot=slot_number pd all show
```

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

```
[root@ixp0301-1a ~]# hpacucli ctrl slot=2 pd all show

Smart Array 6400 in Slot 2
   array A
      physicaldrive 1:0   (port 1:id 0 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:1   (port 1:id 1 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:2   (port 1:id 2 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:3   (port 1:id 3 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:4   (port 1:id 4 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:5   (port 1:id 5 , Parallel SCSI, 300 GB, OK)
      physicaldrive 1:8   (port 1:id 8 , Parallel SCSI, 300 GB, OK)

   array B
      physicaldrive 2:0   (port 2:id 0 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:1   (port 2:id 1 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:2   (port 2:id 2 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:3   (port 2:id 3 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:4   (port 2:id 4 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:5   (port 2:id 5 , Parallel SCSI, 300 GB, OK)
      physicaldrive 2:8   (port 2:id 8 , Parallel SCSI, 300 GB, OK)
```

2. Create the bulkconfig file

a) As a `root` user.
b) Create the `/root/bulkconfig` file.

3. Configure the server hostname

a) Enter the platcfg menu. As `root`, run:

```
# su - platcfg
```

b) Select Server Configuration ➤ Hostname .
c) Click **Edit**.
d) Enter the server hostname in the standard format: ixpNNNN-MA . where:

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

Note: Each subsystem must have the same *NNNN* designation, while the individual server is identified by the *MA* designation (for example, `1A`).

e) Exit the **platcfg** menu.

5.8 Install EFS

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

EFS installation runs from the same CD/ISO as an IXP application. Use IXP CD/ISO for EFS installation. Before you perform this procedure, make sure that you have the appropriate EFS DVD/CD or ISO file available. .

1. **Log in and insert the DVD/CD or distribute the ISO file**

   a) Open a terminal window and log in as `root` on the server you that you want to install the EFS application.

   b) Distribute the media:

   - On the rackmount server insert the EFS DVD/CD or mount the EFS ISO file via iLO (see How to mount the ISO file via iLO).
   - On the c-class blade server download the ISO from the PM&C ISO repository. ISOs are available on the PM&C server under the `/var/TKLC/smac/image` directory. Store the ISO file to `/var/TKLC/upgrade` directory.

2. **Validate the installation media**

   a) Enter the **platcfg** menu. As `root`, run:

   ```
   # su - platcfg
   ```

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

   The validation process must complete without errors. You should receive the following message: CDROM is Valid
   If any errors are reported during this validation process, then **DO NOT USE** this media to install the application.

   d) Exit the **platcfg** menu.

3. **Install the application**

   a) Enter the **platcfg** menu. As `root`, run:

   ```
   # su - platfg
   ```

   b) Select **Maintenance ⊙ Upgrade ⊙ Initiate Upgrade**.
   When the installation process is complete, the server restarts automatically.

   c) If the ISO file was copied to the server, then remove this file to save disk space. As `root`, run:

   ```
   # rm -f /var/TKLC/upgrade/iso_file
   ```

   where *iso_file* is the absolute path of the ISO image, which includes the name of the image.

4. **Analyze the installation log**

   Review the installation log (`/var/TKLC/log/upgrade/upgrade.log`) for any errors.

   If there are any errors, contact the Tekelec Customer Care Center.

5.9 EFS Post-Install Healthcheck

This procedure describes how to run the server healthcheck after the application has been installed on the server.

1. Log in on the server that you want to analyze.
2. As `cfguser`, run:

```
$ analyze_server.sh -p
```

The script gathers the healthcheck information from the server. A list of checks and associated results is generated. There might be steps that contain a suggested solution. Analyze the output of the script for any errors. Issues reported by this script must be resolved before any further use of this server.

The following examples show the structure of the output, with various checks, values, suggestions, and errors.

Example of overall output:

```
[cfguser@ixp8888-1a ~]$ analyze_server.sh
12:40:30: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
12:40:30: date: 08-22-11, hostname: ixp8888-1a
12:40:30: TPD VERSION: 4.2.4-70.90.0
12:40:30: IXP VERSION: [ 7.1.0-64.2.0 ]
12:40:30: XDR BUILDERS VERSION: [ 7.1.0-37.1.0 ]
12:40:30: ------------------------------------------------
12:40:31: Analyzing server record in /etc/hosts
12:40:31:       Server ixp8888-1a properly reflected in /etc/hosts file
12:40:31: Analyzing IDB state
12:40:31:       IDB in START state
12:40:31: Analyzing shared memory settings


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

Example of a successful test:

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

Example of a failed test:

```
12:21:48: Analyzing IDB state
12:21:48: >>> Error: IDB is not in started state (current state X)
12:21:48: >>> Suggestion: Verify system stability and use 'prod.start' to start
 the product
```

After attempting the suggested resolution, if the test fails again, then contact Tekelec Customer Care Center.

5.10 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.

Remount export directories

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

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

c) DataFeed will mount exporting directories back by itself.

5.11 Adjust EFS server

This procedure describes how to adjust the network and other settings accordingly to the bulkconfig file after disaster recovery.

Adjust the server to pre-recovery state

a) Open a terminal window and log in to the recovered server as `root` user.
b) As `root` run:

```
# bc_adjust_subsystem.sh
```

c) Wait until system reconfigures.
d) Verify that the server has been reconfigured correctly.
As `root` run:

```
# bc_customer_integration.sh --post
```

e) If any error occurs contact the Tekelec Customer Care Center.

5.12 Reintegrate EFS with IXP subsystem

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

Reintegrate EFS server with the IXP subsystem

Note: Repeat this step once per each subsystem where this EFS server has been used as Data Export's target before disaster recovery procedure.

a) Such subsystem has already been previously integrated with the EFS server and such the `/root/bulkconfig` file on each IXP server in the subsystem will be already updated with the following line:

```
efs,hostname_of_EFS,IP_address_of_EFS
```

where:

- *hostname_of_EFS* is the hostname of the standalone EFS
- *IP_address_of_EFS* is the IP address of the standalone

EFS For example:

```
efs,ixp7777-1e,10.236.0.33
```

b) Check that such record is present in the `/root/bulkconfig`. Add this record if it's not present. c) As `root` run:

```
# bc_adjust_subsystem.sh
```

d) Wait until system reconfigures. If any problem occurs contact the Tekelec Customer Care Center.

6 Report Server Platform Disaster Recovery Procedure

6.1 Report Server Platform Disaster Recovery Overview

This section describes how to execute a disaster recovery procedure of the Report Server Platform (RSP).

Note: PIC 9.0 release supports only Coupled architecture disaster recovery procedure. Cluster architecture and Decoupled architecture disaster recovery procedures are not supported.

The list of the references below depicts the sequence of procedures that must be executed in sequential order to recover the Report Server Coupled architecture server.

Report Server (RS) Disaster Recovery - Coupled Architecture

Note: Note the entries from /etc/hosts file

1. As root run:

```
# cat /etc/hosts | grep boe-cms
10.240.254.46    ixp0001-1a 1a cms_db_server boe-cms roamacc_rds_db_server
```

Note down aliases, that might be needed after IXP Disaster Recovery..

2. Backup IFR and OFR files. Refer to Backup IFR and OFR files.
3. Execute Disaster Recovery procedure of IXP xDR Storage Server. Skip xDR builder installation and licensing. This is not necessary. Refer to IXP Disaster Recovery Overview.
4. Verify entries in /etc/hosts file. Run

```
# cat /etc/hosts | grep boe-cms
10.240.254.46    ixp0001-1a 1a cms_db_server boe-cms roamacc_rds_db_server
```

If entries as noted during step 1 are not found, add entries for aliases using platcfg menu.

5. Execute Report Server - Coupled Architecture disaster recovery procedure. Refer to Report Server Disaster Recovery (Coupled architecture)
6. Install Analytics Report packages. Install all the analytics report packages that was previously installed before the disaster.Analytics Report packages installation/recovery procedure is not part of this documentation. Follow Analytics Report packages documentation for disaster recovery procedure.
7. Recover IFR and OFR files. Refer to Restore IFR and OFR files.
8. Verify `/etc/hosts` entries on NSP. Refer to Verify RSP host entries in the /etc/hosts file on NSP.

Post Process Service (PPS) Disaster Recovery

1. Execute Disaster Recovery procedure of IXP Base server. Skip xDR builder installation and licensing. This is not necessary.
2. Execute Disaster Recovery procedure for PPS. Refer to PPS Disaster Recovery

6.2 Backup IFR and OFR files

This procedure describes how to backup Input File Repository (IFR) and Output File Repository (OFR)
files on SAP BusinessObjects Enterprise server.

SAP BusinessObjects Enterprise server uses a database schema CMS to store its proprietary data. When a report is run, it reads the report template from the file system called Input File Repository

(IFR), makes a database connection to get the data, formats the report and stores the result of the report instance in the file system called Output File Repository OFR. Since the report output is stored in file system, user can retrieve the report without the need to re-run and access database again.

It is crucial to backup these repository file system, so that it can be used to restore old report instances at a later point of time.

Backup frequency

RSP generates a backup file per day. User should store the generated archive file somewhere else, so that in case of a disaster, the archive file can be used for to recover data later.

Backup directories

Following directories contain the report instances that get backed-up every day at 4:02am. The location of the repository file system differs for the following configurations:

- Rackmount configuration
  - IFR: `/usr/TKLC/oracle/oradata/bobje/frsinput`
  - OFR: `/usr/TKLC/oracle/oradata/bobje/frsoutput`
- VM
  - IFR: `/usr/TKLC/oracle/oradata/IXP/bobje/frsinput`
  - OFR: `/usr/TKLC/oracle/oradata/IXP/bobje/frsoutpu`
- RDS-CMS database version is Oracle 11g
  - IFR: `/var/TKLC/ixp/bobje/frsinput`
  - OFR: `/var/TKLC/ixp/bobje/frsoutput`

Generated archive file

Format of the backup file: *`hostname`*`-`*`day`*`-`*`time`*`-FRS.tgz` (example: `ixp1000-1a-Fri-2011-02-04-FRS.tgz`) where:

- *hostname* is generated by `$(hostname -s)`, example: `ixp1000-1a`
- *day* is generated by `$(date +%a)`, example: `Fri`
- *time* is generated by `$(date +%F)`, example: `2011-02-04`

The generated archive file will be located in the following directory that differs for the following configurations:

- Rackmount configuration: `/usr/TKLC/oracle/oradata/bobje/frs_cms_backup`
- VM: `/usr/TKLC/oracle/oradata/IXP/bobje/frs_cms_backup`
- RDS-CMS database version is Oracle 11g: `/var/TKLC/ixp/bobje/frs_cms_backup`

Backup IFR and OFR files

a) Log in to the Report Server where SAP BusinessObjects Enterprise application is running and copy the archive file to secure location.

6.3 Report Server Disaster Recovery (Coupled architecture)

This procedure describes Report Server application disaster recovery procedure for Coupled architecture. This procedure is based on the fresh install procedure.

Prerequisite: Before you perform this procedure the IXP application must be recovered first. This

server must be recovered with a singl-server IXP subsystem with a designation of 1A, with all parameters the same as before. The IXP application type for Report Server coupled architecture is xDR Storage server. The IXP xDR Storage server bulkconfig file must contain server function `DR-XDR` for disaster recovery procedure.

Continue with the Report Server disaster recovery procedure only after the disaster recovery of IXP xDR Storage server has been completed.

6.3.1 Install Report Server Software

This procedure describes how to install the Report Server software on an IXP server. Before you perform this procedure:

- The server must have an IXP application installed. This server must be a single-server IXP subsystem with a designation of **1A**. Depending on the architecture, the IXP application type is either an xDR storage server or a Base server.
- Make sure that you have the appropriate Report Server DVD/CD or ISO file available.

1. Log in and insert the DVD/CD or mount the ISO file

a) Log in as `root` on the IXP server where you want to install Report Server software. b) Insert the Report Server DVD/CD or distribute the Report Server ISO file to `/var/TKLC/upgrade` directory.

2. Mount the media

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

- For a DVD/CD, enter:

```
# mkdir /media/cdrom
# mount –t auto /dev/cdrom /media/cdrom
```

- For an ISO file, enter:

```
# mount –o loop /var/TKLC/upgrade/REPORT_SERVER_part_number_release_number.iso
 /media
```

where:

- *part_number* is the part number (for example, `872-2121-101`)
- *release_number* is the release number (for example, `9.0.0-9.0.0.3163`)

3. Install the rpm package

a) Install the rpm package. As `root`, run:

- For a DVD/CD, enter:

```
# rpm -ivh /media/cdrom/TKLCrsp-release_number.i386.rpm
```

where *release_number* is the release number (for example, `9.0.0-9.0.0.3163`)

- For an ISO file, enter:

```
# rpm -ivh /media/TKLCrsp-release_number.i386.rpm
```

where *release_number* is the release number (for example, `9.0.0-9.0.0.3163`)

4. Unmount the media

As `root`, run:

- For a DVD/CD, enter:

```
# umount /media/cdrom
# cd
# eject
```

and remove the media from drive.

- For an ISO file, enter:

```
# umount /media
```

and remove the ISO file to save disk space.

6.3.2 Install SAP BOE software on Primary Report Server

This procedure describes how to install the SAP BOE application on an IXP server. Before you perform this procedure:

- The server must have the Report Server application installed.
- Make sure that you have the appropriate SAP BOE DVD/CD or ISO file available.

1. Log in and insert the DVD/CD or mount the ISO file

a) Log in as `root` on the IXP server where you want to install the SAP BOE software.

b) Insert the SAP BOE DVD/CD or distribute the SAP BOE ISO file (for example `boe31_sp3.iso`) to `/var/TKLC/upgrade` directory using the `scp` command. (There will need to be up to 2G space available in this directory.)

c) Verify the media. As `root` run:

```
# md5sum -c boe31_sp3.iso.md5
```

2. Mount the media

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

- For a DVD/CD, enter:

```
# mount –t auto /dev/cdrom /media/cdrom
```

- For an ISO file, enter:

```
# mount –o loop /var/TKLC/upgrade/boe31_sp3.iso /media
```

3. Install BOE

a) As `root`, run:

```
# /var/TKLC/rsp/install.sh
```

b) Choose the server to install:

```
############################################################
#       Installing Report Server Platform 7.1.0-8.1.0      #
############################################################

1) Primary Report Server (Primary RS)
2) Clustered Report Server (Secondary RS)
3) Upgrade Data Aging on all RDS servers.
4) Exit.
>
```

Select 1 to install Primary Report Server.

c) Enter CMS Database IP address or hostname:

```
Please enter CMS Database IP address or hostname:
```

Enter IP address or hostname.

Note: This will depend on the architecture:

- If a Coupled architecture, enter the local IP address.
- If a Decoupled architecture, enter an IP address of the IXP xDR storage server where the CMS database will reside. In this case, it will be the remote IP address. Make sure this server is accessible from the local machine; otherwise, the installation will fail.

d) Enter the Oracle database `sys` user password:

```
Enter Oracle database sys user password:
```

Enter the password.

e) Set the CMC Administrator's password.

This will set the SAP BOE server Central Management Console (CMC) Administrator's password.

```
Please set CMC Administrator's password.
Enter password:
Enter password again:
```

Enter the password, then enter the same password to

confirm. f) Enter the BOE software mount point.

```
Please hit Enter to mount BusinessObject-SP3 CD/DVD ROM or enter a
different mount point [/media/cdrecorder]
```

Press **Enter** for DVD/CD or type `/media` for ISO file.

g) Enter the `root` user password.

```
Enter root os user password:
```

Enter the password.

h) Continue the installation process.

```
Product: BusinessObjects_31_SP3
Installing BusinessObjects Enterprise Server ...   THIS MAKE TAKE SEVERAL
MINUTES!
Check log file /var/TKLC/ixp/boe/setup/logs/BusinessObjects.12.3.log for
internal progress of the BOE server installer.
Please wait...
Checking for recommended patches...

*****************************
Linux: Your system is missing required components (STU00120):
*****************************

Missing patch: unsupported.linux.release

If you continue your installation may not work correctly. (STU00109) Please
press Enter to continue...
```

Press **Enter** to continue.

i) When the installation is complete, check the log file `/var/TKLC/rsp/rsp_install.log` for any errors.

Note: The upgrade may take 30-45 minutes to complete.

If there are any errors, contact the Tekelec Customer Care Center. Example output of a successful installation:

```
Installing Crystal Report Server system service
Restarting all...
Stopping all...
Stopping sian...
Starting all servers...
Starting sian...
Installation Completed Successfully!
```

4. Unmount the media

As `root`, run:

- For a DVD/CD, enter:

```
# umount /media/cdrom
# cd
# eject
```

and remove the media from drive.

- For an ISO file, enter:

```
# umount /media
```

and remove the ISO file to save disk space.

6.3.3 Verify the SAP BOE Primary Server Installation

This procedure describes how to verify that the SAP BOE software is successfully installed on the Primary Report Server before proceeding with the installation process.

1. Open a web browser and go to:

```
http://RS_IP:8080/CmcApp
```

where *RS_IP* is the IP address of the Primary Report Server.

2. Type the IP address of the Primary Report Server in the **System** field.
3. Type `administrator` in the **User Name** field.
4. Enter the **Password** for CMC `administrator` user.
5. Click **Log On**.

If the CMC home page appears, then you were able to log in successfully; the installation of SAP BOE
was successful.

If the home page does not appear, then you were not able to log in and the SAP BOE installation was not successful. Contact the Tekelec Customer Care Center.

6.4 Restore IFR and OFR files

This procedure describes the restore procedure for report instances backup - Input File Repository (IFR) and Output File Repository (OFR) files.

1. Copy the backup file to the Primary Report Server
   a) Open a terminal window and log in as root to the Primary Report Server.
   b) Copy the archive file with the IFR/OFR files backup *hostname-day-time*-FRS.tgz (example: ixp1000-1a-Fri-2011-02-04-FRS.tgz) to the / directory using scp.
2. Restore the backup a) As root run:

```
# tar -xzvf  hostname-day-time-FRS.tgz
```

example:

```
# tar -xzvf  ixp1000-1a-Fri-2011-02-04-FRS.tgz
```

Note: Archive file is automaticaly created in frs_cms_backup folder. Documents scheduled after an archive's creation can not be bundled in that archive. Consequently, on backing up the archive after a disaster, some report documents (scheduled after the archive creation), will possibly be lost. On opening such documents, the user will get the following error: **The document can't be retrieved from the File Repository Server. Please contact your BusinessObjects administrator.(Error: WIS 30951) (Error: INF)**

6.5 Verify RSP host entries in the /etc/hosts file on NSP

This procedure describes how to verify RSP host entries in the /etc/hosts file on NSP server.
Note: Run this procedure on NSP One-Box server or repeat this procedure on all NSP servers that are part of Four-Box setup.

Verify /etc/hosts on NSP

a) Open a terminal window and log in as root on the NSP server.
b) As root run:

```
# cat /etc/hosts
```

The output must contain an alias entry boe-cms for recovered Report Server IP address.
c) If the boe-cms alias is missing update the /etc/hosts file via platcfg and add this alias for recovered Report Server IP address.

6.6 PPS Disaster Recovery

6.6.1 Install PPS Application

This procedure describes Post Process Service (PPS) disaster recovery procedure. This procedure is based on PPS fresh install procedure.

Prerequisite: Before you perform this procedure the IXP application must be recovered first. The IXP application type for PPS service is IXP Base server and such server is part of the IXP subsystem. The IXP Base server bulkconfig file must contain server function DR-BASE for disaster recovery procedure. Continue with the PPS disaster recovery procedure only after the disaster

recovery of IXP Base server, where the PPS server is running, has been completed.

This procedure describes how to install the PPS application.

Before you perform this procedure, make sure that the IXP Base server, where PPS will be installed, is part of an existing IXP subsystem

1. **Log in and either insert the DVD/CD or distribute the ISO file**
   a) Log in as `root` on the server.
   b) Insert Network Intelligence DVD/CD or distribute the ISO file via iLO.

2. **Mount the media**

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

   - For a DVD/CD, enter:

     ```
     # mkdir /media/cdrom
     # mount –t auto /dev/cdrom /media/cdrom
     ```

   - For an ISO file, enter:

     ```
     # mount –o loop /usr/RS-PPS_part_number_release_number.iso /media
     ```

     where:

     - *part_number* is the part number (for example, `872-2121-101`)
     - *release_number* is the release number (for example, `9.0.0-9.0.0.3163`)

3. **Install the rpm package**

   As `root`, run:

   - For a DVD/CD, enter:

     ```
     # rpm -ivh /media/cdrom/TKLCpps-release_number.i386.rpm
     ```

   - For an ISO file, enter:

     ```
     # rpm -ivh /media/TKLCpps-release_number.i386.rpm
     ```

     where:

     - *release_number* is the release number (for example, `9.0.0-9.0.0.3163`)

4. **Unmount the media**

   As `root`, run the appropriate command depending on the mount point used:

   - For a DVD/CD, enter:

     ```
     # umount /media/cdrom
     ```

   - For an ISO file, enter:

     ```
     # umount /media
     ```

5. **Shutdown PPS**

   Login as cfguser and execute the command

   ```
   cd /var/TKLC/ixp/pps
   ```

   ```
   ./pps shutdown
   ```

6. **Restore the XMLs**

Execute the below command to restore the xmls

If the directory does not exist, than create the directory using cfguser

```
mkdir
/var/TKLC/ixp/pps/thirdparty/Knopflerfish_2_0_5/knopflerfish.org/osgi/xml/
```

Restore the XMLs using root user

```
scp -r root@<IP>:/var/TKLC/ppsxmls/*
/var/TKLC/ixp/pps/thirdparty/Knopflerfish_2_0_5/knopflerfish.org/osgi/xml/
chown cfguser:cfg
/var/TKLC/ixp/pps/thirdparty/Knopflerfish_2_0_5/knopflerfish.org/osgi/xml/
```

Where <IP> is the IP address of the system on which backup is saved before disaster recovery.

7. **Start PPS**

```
cfguser# cd /var/TKLC/ixp/pps./pps startup
```

6.6.2 Post Installation Verification

This procedure describes how to verify the PPS installation.

1. **Connect to Knopflerfish OSGi Framework using the remote console**

a) Log in as `cfguser` on the PPS server.

b) Connect to the Knopflerfish OSGi Framework console. As `cfguser`, run:

```
$ telnet localhost 2323
```

Example output:

```
Verification Connected to localhost.
Escape character is '^]'.
Knopflerfish OSGi console
login: admin
password: admin
'quit' to end session
```

c) Enter the username (`admin`) and the associated password.

2. **Verify the registered services**

a) Check the list of registered services. Run:

```
> services
```

If the `initconfig-manager` service appears as registered, then the installation is successfull. Example output:

```
Bundle: initconfig-manager-LIB (#26)
registered: DtsConsumer InitConfigManagerService
[DelegatedExecutionOsgiBundleApplicationContext,
ConfigurableOsgiBundleApplicationContext,
ConfigurableApplicationContext, ApplicationContext, Lifecycle,
ListableBeanFactory,
HierarchicalBeanFactory, MessageSource, ApplicationEventPublisher,
ResourcePatternResolver,
BeanFactory, ResourceLoader, DisposableBean]
```

Note: In addition to the `initconfig-manager` service, the following services also appear as registered after RDM reporting package is installed on a Primary RS and discovered in CCM.

```
Bundle: oam-service-LIB
Bundle: pps-manager-LIB
Bundle: process-LIB
Bundle: referencedata-service-LIB
Bundle: translator-service-LIB
```

b) Exit the console. Run:

```
> quit
```

7 PIC IP Changes Procedure

7.1 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.

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**

   Note: Execute this step if you are going to migrate NSP One-Box or NSP Four-Box to new network settings, else skip.

   a) Refer to NSP IP Change Procedure

3. **xMF IP Change Procedure**

   Note: Execute this step if you are going to migrate xMF(s) to new network settings, else skip.

   - For TODO refer to XMF subsystem IP Change Procedure for TPD3
   - For TODO refer to XMF subsystem IP Change Procedure for TPD5

4. **IXP IP Change Procedure**

   Note: Execute this step if you are going to migrate IXP(s) to new network settings, else

   skip. a) Refer IXP Subsystem IP Change Procedure

5. **EFS IP Change Procedure**

   Note: Execute this step if you are going to migrate Export File Server(s) (EFS) to new network settings, else skip.

   a) Refer to Export File Server 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.
   f) Repeate steps c-e for all affected feeds.

7. **RSP IP Change Procedure**

Note: Execute this step if you are going to migrate Report Server Platform (RSP) to new network settings, else skip.

a) Refer to Report Server IP Change Procedure

7.2 NSP IP Change Procedure

This procedure describes the NSP IP change procedure.

1. Refer to Modify NSP One-Box IP Addressfor changing IP address of OneBox.
2. Refer to Modify NSP Apache IP Address (Four-Box Configuration)for changing IP address for Apache Server.
3. Refer to Modify NSP Secondary or Oracle IP Address (Four-Box Configuration)for changing IP addresses of Oracle Server or weblogic secondary.
4. Refer to Modify NSP Primary IP Address (Four-Box Configuration)for changing the IP address of Weblogic primary.
5. Refer to Update NSP IP addresses on xMF (TPD3)for updating NSP IP addresses on XMF subsystem (TPD 3.X).
6. Refer to Update NSP IP addresses on xMF (TPD4) for updating NSP IP addresses on XMF subsystem (TPD 4.X).
7. Refer to Update NSP IP addresses on IXP or EFS for updating NSP IP addresses on IXP subsystem or EFS servers

7.2.1 Modify NSP One-Box IP Address

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

1. Open a terminal window and log in as `root` on the NSP One-Box server.
2. Enter the **platcfg** menu. As `root`, run:
```
# su - platcfg
```
3. Select **Network Configuration ⊙ Network Interfaces ⊙ IPv4 ⊙ Edit an Interface** .
4. Select the appropriate interface option and click **OK**:
   - **eth01** for rackmount
   - **bond0.3** for blade
5. Select **OK** and press **Enter**.
6. Select Boot Protcol as **none** and press **ENTER**
7. Choose Address Action as **edit** and press **ENTER**
8. Type the new IP address for this interface and the netmask, if needed.

Note: Update the netmask only if different from the original setting.

9. Select **OK** and press **Enter**. Then navigate back to the **platcfg** main menu.
10. Repeat steps 3–7 for the second interface. Use the appropriate option:
    - **eth02** for rackmount

- **bond0.4** for blade

11. Select Boot Protcol as **none** and press **ENTER**

12. Choose Address Action as **edit** and press **ENTER**

13. From main **platcfg** menu, select **Network Configuration ⊙ Routing ⊙ IPv4 ⊙ Static Routes ⊙** Display Table ⊙ main ⊙ Edit ⊙ Edit Route ⊙ default.

14. Select the route to edit. Then select **Type** as default and click **OK**.

15. Type the new gateway IP address and click **OK**.

16. Click **Exit** until the main **platcfg** menu appears.

17. If the second interface gateway IP address needs to be modified, repeat steps 9–12 for the second interface (either **eth02** or **bond0.4**).

18. From the main **platcfg** menu, select **NSP Configuration ⊙ IP Configuration**.

19. Click **Edit**.

20. Click **Yes**.
The IP address is changed.

21. Exit the **platcfg** menu.

22. After the IP address is changed , run the below command as a `root` user

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

where *new_onebox_ip* will be the new IP address of NSP server.

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

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

1. Open a terminal window and log in as `root` on the NSP Apache server.

2. Enter the **platcfg** menu. As `root`, run:

```
# su – platcfg
```

3. Select **Network Configuration ⊙ Network Interfaces ⊙ Edit an Interface** .

4. Select the appropriate interface option and click **Edit**:

- **eth01** for rackmount
- **bond0.3** for blade

5. Select **No** and press **Enter** when asked to configure the MTU.
6. Select **No** and press **Enter** when asked to configure the GRO.

7. Select **Yes** and press **Enter** when asked to configure the Boot Protcol.
8. Select Boot Protcol as **none** and press **ENTER**
9. Choose Address Action as **edit** and press **ENTER**

10. Type the new IP address for this interface and the netmask, if needed.

Note: Update the netmask only if different from the original setting.

11. Select **OK** and press **Enter**. Then navigate back to the **platcfg** main menu.

12. Repeat steps 3–7 for the second
interface. Use the appropriate option:

- **eth02** for rackmount
- **bond0.4** for blade

13. Select Boot Protcol as **none** and press **ENTER**

14. Choose Address Action as **edit** and press **ENTER**
15. From main **platcfg** menu, select **Network Configuration ⊙ Routing ⊙ IPv4 ⊙ Static Routes ⊙** Display Table ⊙ main ⊙ Edit ⊙ Edit Route ⊙ default.
16. Select the route to edit. Then select **Type** as default and click **OK**.
17. Type the new gateway IP address and click **OK**.
18. Click **Exit** until the main **platcfg** menu appears.
19. If the second interface gateway IP address needs to be modified, repeat steps 9–12 for the second interface (either **eth02** or **bond0.4**).
18. From the main **platcfg** menu, select **NSP Configuration ⊙ IP Configuration**.
19. Click **Edit**.
20. Type the new IP addresses for the NSP Primary and NSP Secondary in the appropriate fields and click **OK**.
21. Press **Enter**.
    A confirmation prompt appears.
22. Click **Yes**. This step will finalize NSP Apache IP change procedure. Leave the **platcfg** menu.

7.2.3 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.

1. Open a terminal window and log in as `root` on the NSP Secondary server or NSP Oracle server.
2. Enter the **platcfg** menu. As `root`, run:
   ```
   # su – platcfg
   ```
3. Select **Network Configuration ⊙ Network Interfaces ⊙ IPv4 ⊙ Edit an Interface** .
4. Select the appropriate interface option and click **OK**:
   - **eth01** for rackmount
   - **bond0.3** for blade
5. Select **OK** and press **Enter**.
6. Select Boot Protcol as **none** and press **ENTER**
7. Choose Address Action as **edit** and press **ENTER**
8. Type the new IP address for this interface and the netmask, if needed.

   Note: Update the netmask only if different from the original setting.
9. Select **OK** and press **Enter**. Then navigate back to the **platcfg** main menu.
10. From main **platcfg** menu, select **Network Configuration ⊙ Routing ⊙ IPv4 ⊙ Static Routes ⊙** Display Table ⊙ main ⊙ Edit ⊙ Edit Route ⊙ default.
11. Select the route to edit. Then select **Type** as default and click **OK**.
12. Type the new gateway IP address and click **OK**.
13. Click **Exit** until the main **platcfg** menu appears.
14. From the main **platcfg** menu, select **NSP Configuration ⊙ IP Configuration**.
15. Click **Edit**.
16. Click **Yes**.
    The IP address is changed.
17. Exit the **platcfg** menu.

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

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

1. Open a terminal window and log in as `root` on the NSP Primary server.
2. Enter the **platcfg** menu. As `root`, run:
   ```
   # su – platcfg
   ```
3. Select **Network Configuration ⊙ Network Interfaces ⊙ IPv4 ⊙ Edit an Interface** .
4. Select the appropriate interface option and click **OK**:
   - **eth01** for rackmount
   - **bond0.3** for blade
5. Select **OK** and press **Enter**.
6. Select Boot Protcol as **none** and press **ENTER**
7. Choose Address Action as **edit** and press **ENTER**
8. Type the new IP address for this interface and the netmask, if needed.

   Note: Update the netmask only if different from the original setting.
9. Select **OK** and press **Enter**. Then navigate back to the **platcfg** main menu.
10. From main **platcfg** menu, select **Network Configuration ⊙ Routing ⊙ IPv4 ⊙ Static Routes ⊙** Display Table ⊙ main ⊙ Edit ⊙ Edit Route ⊙ default.
11. Select the route to edit. Then select **Type** as default and click **OK**.
12. Type the new gateway IP address and click **OK**.
13. Click **Exit** until the main **platcfg** menu appears.
14. From the main **platcfg** menu, select **NSP Configuration ⊙ IP Configuration**.
15. Click **Edit**.
16. Type the new IP addresses for the NSP Apache, NSP Oracle, and NSP Secondary servers in the appropriate fields and click **OK**.
17. Press **Enter**.
    A confirmation prompt appears.
18. Click **Yes**. This step will finalize NSP Apache IP change procedure. Leave the **platcfg** menu.
19. After the IP address is changed , run the below command as a root user
    ```
    # su - cfguser -c "setCCMnode new_oracle_ip"
    ```
    where *new_oracle_ip* will be the IP address of new oracle server.

7.2.5 Update NSP IP addresses on xMF (TPD3)

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

Configure the NSP application server's IP address.

a) Log in as `root` on 1A (0A in case of standalone) server.

b) Run setAppServer script
```
# /usr/TKLC/TKLCmf/bin/setAppServer

Please enter an IP address for appserver:
```

c) Enter IP address of the weblogic primary server

Output should be similar to below(if there is only "Does the system have a 2nd Application Server (y or n) ? " it is correct too):
```
XX.XX.XX.XX         appserver
```

```
Old appserver entry not found.  Adding
RCS_VERSION=1.X
Updating hosts.byname...
Updating hosts.byaddr...
Does the system have a 2nd Application Server (y or n) ?
```

d) For set the ip of the weblogic secondary server answer **y** otherwise **n.**
If you do not want to set weblogic secondary server answer **n:**

```
#
```

If you want to set weblogic secondary server answer **y**:

```
Please enter an IP address for appserver2:
```

Enter IP address of the weblogic secondary server

```
Updating hosts.byname...
Pushing hosts.byname map to blue-1b ...
Updating hosts.byaddr...
Pushing hosts.byaddr map to blue-1b ...
#
```

e) Reboot 1A (or 0A in case of standalone) server
f) After 1A(0A) server is completely rebooted reboot all non-1A servers.

Note: Skip this step for standalone

7.2.6 Update NSP IP addresses on xMF (TPD4)

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

Configure the NSP application server's IP address.

Note: This step is run on all servers in the subsystem and on standalone

server. a) Login as `root` on the server
b) Update appservers in `/var/TKLC/upgrade/platform.csv` file with appropriate values.
c) Run bulkconfig script:

```
# bulkConf.pl
```

Example of correct output:

```
Name: tek3-1a
Func: IMF
Desig: 1A
Cust: bond0.200
HostIp: 10.236.2.69
Mask: 255.255.255.224
```

```
Route: 10.236.2.65
LiveIP: 10.236.2.69... NTP: ntpserver1
Ip: 10.0.1.11
APP: appserver
Ip: 10.236.2.134
Deleting appserver10.236.2.133...
Adding new appserver 10.236.2.134...
TZ: Europe/Prague
```

d) Reboot the server.

7.2.7 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 assume 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.

Update bulkconfig and adjust the subsystem/EFS.

a) Open a terminal window and log in on any server in the IXP subsystem or EFS as `root`.
b) Update the `/root/bulkconfig` file with the new NSP IP addresses.
c) Adjust the IXP subsystem/EFS. As `root` run:

```
# bc_adjust_subsystem.sh
```

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

7.3 XMF subsystem IP Change Procedure for TPD3

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

1. Change IP

a) As root enter platcfg configuration menu:

```
# su - platcfg
```

b) Navigate to **Network Configuration ⊙ Configure Subnets Network Interfaces**
c) Edit the **cust** network IP address of the frame (**not the IP address of the XMF!**) and its netmask

2. Edit default route.

Note: There should be only one default route after the default route configuration is finished.

a) Navigate to **Network Configuration ⊙ Routing ⊙ Edit ⊙ Edit Route**
b) Select **default** route menu, confirm **default** by **OK.**
c) Select **Device** and edit **Gateway.**

Possible interfaces:

- eth81.200 for Tekserver 1
- eth91.200 for Tekserver 2
- eth01.200 for Tekserver 3 and DL380 G5
- eth41.200 for HP ML350 G5
- bond0.200 if `REDUNDANT WAN` is enabled

d) Select **Exit** and press `<ENTER>` repeatedly until you are back to the **Main Menu**

3. Reboot the 1A server a) Reboot 1A server. As root run:

```
# reboot
```

Note: The reboot may take up to 15 minutes while the MRV (Tekserver 1 systems only), and/or
Switches are being updated.

4. Reboot all non-1A servers.

a) After 1A server is completely rebooted reboot all non-1A servers.

As root run:

```
# reboot
```

5. **Edit default route for all non-1A servers.**

Note: There should be only one default route after the default route configuration is finished.

a) Navigate to **Network Configuration ⊙ Routing ⊙ Edit ⊙ Edit Route**

b) Select **default** route menu, confirm **default** by **OK.**

c) Select **Device** and edit **Gateway.**

Possible interfaces:

- eth81.200 for Tekserver 1
- eth91.200 for Tekserver 2
- eth01.200 for Tekserver 3 and DL380 G5/G6
- eth41.200 for HP ML350 G5
- bond0.200 if `REDUNDANT WAN` is enabled

d) Reboot the server. As root run:

```
# reboot
```

6. **Change VIP address and start it.**

Note: This is run on the primary server only.

a) Login to **primary** server as **cfguser**

b) 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

Example of output:

```
Change VIP from 192.168.14.31 to 192.168.14.35, are you sure? (y/n)y
VIP in StringParam is updated to 192.168.14.35
Stop the previous VIP 192.168.14.31
VIP in DaqSubSystem is updated
```

7. **Change the IP address of XMF subsystem in NSP**

a) From Internet Explorer, connect to the NSP Application GUI using the following URL: *http://192.168.1.1/nsp*

Where **192.168.1.1** is the IP address of the Weblogic Primary Server

Note: Replace **192.168.1.1** by actual IP address of the Weblogic Primary Server.

b) Login to the Application with User name " **tekelec**"

c) Go to CCM Application

d) Navigate to **Equipment Registry** in Left Tree

Panel. e) click on **Subsystem**

f) Modify the servers and change Admin IP address field to the new IP address

8. **Discover xMF Applications in NSP and check VIP**

   a) Navigate to **Equipment Registry** in Left Tree Panel. b) Select site name
   c) Select **XMF ⊙ xMF Subsystem**
   d) use button to **Discover applications** of **primary** server only!
   e) Check if the VIP address is correctly updated for xMF subsystem :
   f) Click on **XMF**
   g) in Right Panel check **Virtual IP Address**
      If Virtual IP Address is not updated discover applications of primary server again.
   h) **Apply Changes** on xMF.

9. **Apply changes on the IXP**

   a) Apply changes on the IXP subsustems connected to the xMF subsystem

10. **Check connection between xMF and IXP in NSP**

    a) Check connection between xMF and IXP in NSP

7.4 XMF subsystem IP Change Procedure for TPD5

Use this procedure to change IP addresses of an XMF Subsystem with TPD4 or more only.

1. **Change IP**

Note: Repeat this step on all servers in the subsystem!

a) Login as `root` on the server
b) Update `/var/TKLC/upgrade/platform.csv` file with appropriate values.
c) Run bulkconfig script:

```
# bulkConf.pl
```

Example of correct output:

```
Name: imf-1a
        Func: IMF
        Desig: 1A
        Cust: bond0.200
        HostIp: 192.168.253.5
        Mask: 255.255.255.224
        Route: 192.168.253.1
        Updating hostname to imf-1a.
        LiveIP: 192.168.253.5...
NTP: ntpserver1
        Ip: 10.250.32.10
        Updating ntpserver1...
NTP: ntpserver2
        Ip: 10.250.32.11
        Updating ntpserver2...
NTP: ntpserver3
        Ip: 10.250.32.12
        Updating ntpserver3...
NTP: ntppeerA
        Ip: 10.250.32.13
        Updating ntppeerA...
NTP: ntppeerB
        Ip: 10.250.32.14
```

```
        Updating ntppeerB...
APP: appserver
        Ip: 10.10.10.10
        Adding new appserver...
APP: appserver2
        Ip: 10.10.10.11
        Adding new appserver...
TZ: Europe/Prague
        Updating Timezone America/New_York to Europe/Prague...
```

d) Reboot the server.

2. Change VIP address and start it.

Note: This is run on the primary server only.

a) Login to **primary** server as **cfguser**

b) 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

Example of output:

```
Change VIP from 192.168.14.31 to 192.168.14.35, are you sure? (y/n)y
VIP in StringParam is updated to 192.168.14.35
Stop the previous VIP 192.168.14.31
VIP in DaqSubSystem is updated
```

3. Change the IP address of XMF subsystem in NSP

a) From Internet Explorer, connect to the NSP Application GUI using the following URL:
http://192.168.1.1/nsp
Where **192.168.1.1** is the IP address of the Weblogic Primary Server

Note: Replace **192.168.1.1** by actual IP address of the Weblogic Primary

Server. b) Login to the Application with User name " **tekelec**"

c) Go to CCM Application

d) Navigate to **Equipment Registry** in Left Tree

Panel.

e) click on **Subsystem**

f) Modify the servers and change Admin IP address field to the new IP address

4. Discover xMF Applications in NSP and check VIP

a) Navigate to **Equipment Registry** in Left Tree

Panel. b) Select site name

c) Select **XMF ⊙ xMF Subsystem**

d) use button to **Discover applications** of **primary** server only!

e) Check if the VIP address is correctly updated for xMF subsystem :

f) Click on **XMF**

g) in Right Panel check **Virtual IP Address**

If Virtual IP Address is not updated discover applications of primary server again.

h) **Apply Changes** on xMF.

5. **Apply changes on the IXP**

   a) Apply changes on the IXP subsustems connected to the xMF subsystem

6. **Check connection between xMF and IXP in NSP**

   a) Check connection between xMF and IXP in NSP

7.5 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 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`run:

   ```
   # bc_changeip_subsystem.sh
   ```

   You will be prompted to confirm this operation. Type `yes` and press `<enter>`.

   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.

   If you are migrating across the network, continue to the next substep.

   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.

   g) Change IXP subsystem VIP address. Login to the ActMaster server of the IXP subsystem as `cfguser`.

As `cfguser` run:

```
$ setCcmIp nsp_oracle_ip VIP
```

where *nsp_oracle_ip* is the IP address of the NSP Oracle server (Four-box) or NSP One-box server and *VIP* is the new VIP address of the IXP subsystem. The VIP address is the address that is in the same subnet and is not assigned to any server.

3. Change IXP subsystem IPs in NSP

a) Login to the NSP GUI and navigate to CCM.
b) Navigate to **Equipment Registry**.
c) Click on **Subsystem**.
d) Modify the servers and change **Admin IP address** field to the new IP address

4. Apply changes

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

7.6 Export File Server IP Change Procedure

This procedure describes how change the IP settings on the Export File Server (EFS). 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 of Standalone Export Server you are about to reconfigure.
b) Update the `/root/bulkconfig` file with the new IP address.

2. Run IP change

a) Run the Export File Server IP change procedure. As `root`run:

```
# bc_changeip_standalone.sh
```

You will be prompted to confirm this operation. Type `yes` and press `<enter>`.

b) The EFS server 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) The server will be rebooted at the end of the procedure.

e) If you migrate across the network then after the reboot perform any HW configuration like cabling etc. to make the server accessible in the new settings.

3. Update new EFS IP address on IXP servers

a) Log in to the rebooted EFS server as `root` and run:

```
# bc_changeip_standalone.sh --finish
```

The IP address of EFS server will be updated on all associated IXP subsystems.

4. Change EFS IP in NSP

a) Login to the NSP GUI and navigate to CCM.

b) Navigate to **Equipment Registry**.

c) Click on **site** with Standalone Export Server. Click on **EFS** and then on you subsystem. d) Modify the servers and change **Admin IP address** field to the new IP address

7.7 Report Server IP Change Procedure

This procedure describes how change the IP settings on the Report Server (RS). 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 of Report Server you are about to reconfigure.

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

2. Run IP change

a) Run the Report Server IP change procedure. As `root` run:

```
# bc_changeip_subsystem.sh
```

You will be prompted to confirm this operation. Type `yes` and press `<enter>`.

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) Ignore the following message:

```
Error: Oracle is running but problems occured
```

e) 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.

If you are migrating across the network, continue to the next substep.

f) Perform any hardware related configuration like cabling etc.

g) Log in back to the server 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. Update DaqServer IP address

a) Login to the Report Server as
`cfguser`. b) As `cfguser` run:

```
$ itrunc DaqServer
$ echo "$HOSTNAME|$(hostname -i)|ActMaster|REPORT" | iload -f_name -f_address
 -f_role -f_ssId DaqServer
```

Verify that the IP address of DaqServer has been changed:

```
$ iqt -phz -f_address DaqServer where "_name='$HOSTNAME'"
```

4. Update Report Package IP address

Note: Run this step if the report packages has been

installed. a) Login to the Report Server as `root`.

b) Edit the `RSPPackageInfo.xml` file with `vi` editor. As `cfguser` run:

```
$  vi /usr/TKLC/TKLCjmxagent/in/RSPPackageInfo.xml
```

Update the IP address only for those report packages that are installed on this server in the `<ReportDataServer>` tag section. Example:

```
<ReportDataServers>
<host packageid="sigtran_trans" hostname="sigtran_trans_rds_db_server"
hostaddress="10.250.54.252" />
<host packageid="tdm_call" hostname="tdm_call_rds_db_server"
hostaddress="10.250.54.252" />
<host packageid="roamacc" hostname="roamacc_rds_db_server"
hostaddress="10.250.54.252" />
</ReportDataServers>
```

5. Refresh Report Server IP address

a) Refresh Report Server IP address by running install script. As `root` run:

```
$ /var/TKLC/rsp/install.sh
```

Move along and answer the prompt questions.

6. Change Report Server IPs in NSP

a) Login to the NSP GUI and navigate to CCM.

b) Navigate to **Equipment Registry**.

c) Click on **site** with your Report Server.

d) Click on **Report Server**.

e) Click on your subsystem and modify the servers and change **Admin IP address** field to the new
IP address.

f) Select the server and click on **Discover Applications**.

g) Verify that **ReportInfoView** is accessible. Navigate to **Home**. Click on **ReportInfoView** application. If the **ReportInfoView** is not accessible restart the NSP server. Open a terminal window and log in to NSP One-Box or Primary and Secondary NSP server (Four-Box) as `root` user. Restart NSP service. As `root` run:

service nspservice restart

8 PIC Hardware Migration Procedures

8.1 Migrate NSP DL360 G5 Server to DL360 G6 Server (Optional)

Follow this procedure to migrate DL360 G5 servers to DL360 G6 servers. This step is optional prior to NSP 9.0 major upgrade procedure.

1. **Take Backup**

   a) Take Backup of NSP Database Backup and Realm Backup

2. **Install G6 server**

   a) Replace the NSP server (earlier G5) by the G6 server

3. **Perform Disaster Recovery on server.**

   a) After replacing with new G6 hardware, perform disaster recovery on this box using *NSP Disaster Recovery Procedures* .

8.2 Migrate IXP DL360/DL380 G5 Server to DL360 G6 Server

This describes how to migrate the HP G5 hardware to HP G6 hardware

HP G5 hardware is supported on PIC 9.0 release. Thus it's assumed that the IXP subsystem has already been upgraded to 9.0 prior executing this procedure.

This procedure will guide you through the following highlevel steps:

- Backup the KPI sessions
- Integrate G6 server to IXP subsystem
- Offload G5 server to G6 server
- Remove G5 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 this 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-f fo each KPI session you want to backup.

2. **Integrate G6 server to IXP subsystem**

a) Run PIC 9.0 manufacturing installation for the HP G6 server.

b) Add this server to IXP 9.0 subsystem that contains the HP G5 server you are about to replace.

3. Offload G5 server to G6 server

a) From NSP GUI move all DFPs assigned to HP G5 server to new HP G6 server.

4. Put IXP G5 xDR Storage server to read-only mode

Note: This step is applicable to xDR Storage server only. IXP G5 xDR Storage server must be excluded from the xDR Storage Pool.

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 xDR Storage Servers will be displayed.
d) Mark the IXP G5 xDR server as `QUERY_ONLY`.

5. Disable G5 PDU Storage server write permission

Note: This step is applicable to PDU Storage server only. IXPG5 PDU Storage server must be exluded from PDU Storage Pool.

a) Open a terminal window and log in to IXP G5 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 G5 server has no valid data

a) Wait as long as G5 server has any valid data. Once the session expired (in case of xDR Storage server), or PDUs will be purged (in case of PDU storage server) you can continue with the rest of the procedure.

7. Remove IXP G5 server from the IXP subsystem.

a) The whole IXP G5 server functionality has been now replaced with G6 server. Remove the IXP G5 server from the IXP subsystem.

8. Import KPI sessions to IXP 9.0 subsystem

Note: Now you can import all the KPI sessions you have exported before the G4p->G6 HW migration. 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 that you want to import are configured.
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:

```
Session name: <session>
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.
```

9 NSP Maintenance Procedures

9.1 NSP Upscale Procedure

9.1.1 NSP Pre-Upscale Sanity Tests

This procedure describes different steps for sanity check before Upscale

1. **WebLogic Console**
   a) From Internet Explorer, connect to the WebLogic console using the following URL:
   http://nsp_ip:8001/console

   where `nsp_ip` is the IP address of the NSP One-Box server or NSP Primary WebLogic server (Four-Box).
   b) Login with user `weblogic`
2. **Health Check**
   a) Under the **Environment** heading, click on the **Servers** link
   b) The console would display the **Summary of Servers**, with a list of the three servers, nsp1a, nsp1b and nspadmin.
   c) Entries in the columns **State** and **Health** should be **RUNNING** and **OK** for all three servers.
3. **NSP GUI**
   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 `tekelec`
4. **Build Verification**
   a) In the top frame, on mouse-over on the link **Portal**, click on the **About** link that will be displayed. A pop-up window with the build information will be displayed.
   b) The build version should display `Portal 9.0-X.Y.Z`.

   Where 9.0-X.Y.Z should be the new build number.

9.1.2 NSP Pre-Upscale Steps

This procedure describes different steps to be followed before running upscale procedure.

1. **Prepare Apache Box**
   a) Follow the steps below to install the Operating System.

- For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
- For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
- For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers

- For C-class blade follow IPM Blade Servers Using PM&C Application

2. Prepare Secondary Box

a) Follow the steps below to install the Operating System.

- For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
- For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
- For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
- For C-class blade follow IPM Blade Servers Using PM&C Application

3. Prepare Primary Box

a) Follow the steps below to install the Operating System.

- For RMs HP G5 server follow Install Operating System on G5 Rackmount Servers
- For RMs HP G6 server follow Install Operating System on G6 Rackmount Servers
- For RMs HP Gen8 server follow Install Operating System on Gen8 Rackmount Servers
- For C-class blade follow IPM Blade Servers Using PM&C Application

4. Prepare Oracle Box

a) Oracle box in a Four Box NSP Cluster will have only one IP Address.
Follow the procedure *How to remove IP Address and Route*.

5. Verify /tekelec does not exist

a) Login as `root` user on the Primary Box (The box which would be finally Primary Box)
b) Verify that **/tekelec** does not exist by using the command.
As root run:

```
# df /tekelec
```

if it shows `/usr` partition then it is ok else follow the following steps. As root run:

```
# rm –rf /tekelec
```

9.1.3 NSP Upscale One Box to Four Box

This procedure describes different steps to be followed for upscale from NSP One-Box to NSP Four-Box configuration.

1. Login

a) Open a terminal window and log in as `root` on the original NSP One-Box server.

2. Upscale NSP Oracle server

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

```
# su – platcfg
```

b) Navigate to **NSP Configuration ⊙ Upscale** and press `<enter>`.
c) Provide IP address for NSP Primary WebLogic, NSP Secondary WebLogic and NSP Apache server. Select the radio button `yes` for purging terminated alarms and purging all alarms.
d) Select **OK** and press `<enter>`

3. **Upscale NSP Apache server**

a) Complete the NSP Apache server installation by following the steps for NSP Pre-Install Configuration and then Install NSP

4. **Upscale NSP Secondary WebLogic server**

a) Complete the Weblogic Secondary Box installation by following the steps for NSP Pre-Install Configuration and then Install WebLogic

5. **Upscale NSP Primary WebLogic server**

Note: Step b and step c are crucial and MUST NOT be omitted! Omitting this step WILL result in data loss.

a) Login as `root` user on the NSP Primary WebLogic server on a Four-Box setup b) Create `/opt/recovery` file.

As `root` run:

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

c) Copy the optional modules list file from backup at earlier NSP One-Box (now NSP Oracle) into `/tmp` of NSP Primary WebLogic (Four-Box).

E.g. Run following command from earlier onebox (before upscale). As `root` run:

```
# scp nsp_oracle_ip:/opt/oracle/backup/upgrade_backup/optional_modules_list
/tmp
```

where *nsp_oracle_ip* is the IP address of NSP Oracle (Four-box, previously One-Box server)

d) Complete installation by following the remaining steps for the weblogic primary server only.

Follow NSP Pre-Install Configuration, then Install WebLogic and then Install NSP

e) Copy the realm backup folder exportrealm from Oracle Box `/opt/oracle/backup/upgrade_backup/exportrealm/` into a local directory in the primary box.

f) Restore the realm. As `root` run:

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

where *backup_dir*contains the backup of realm data.

6. **Remove the A-Node from NSP Oracle server**

Run this step on original NSP One Box (now NSP Oracle server) to remove the A-Node. As `root` run:

```
# su - cfguser -c prod.dbdown
# rpm -e --noscripts TKLCmf
# rpm -e comcol-mysql
# rpm -e comcol
# rpm -e TKLCdbreplicator
```

7. **Installation logs**

a) Installation log is available at `/var/log/nsp/install/nsp_install.log`

8. **Install the A-Node on NSP Primary WebLogic server**

a) Open a terminal window and log in on NSP Primary Web-Logic serveras `root`

b) Insert the XMF CD to the cdrom

c) If ISO is available copy the iso to NSP primary server at some location.

d) 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`)

e) Type **yes** to confirm

f) No reboot need

9. Deploy scheduler queues

a) Login as tekelec user on the terminal console and execute following commands. As `tekelec` run:

```
$ cd /opt/nsp/nsp-package/protraq
$ ant deploy.scheduler.queue
$ cd /opt/nsp/nsp-package/protrace
$ ant deploy.scheduler.queue
$ cd /opt/nsp/nsp-package/forwarding
$ ant jms.deploy
```

NOTE (WORKAROUND PR 216438) :: - During NSP Upscale at the end user need to apply following workaround in order to deploy missing application

Login as tekelec user on NSP primary box

```
$ 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
```

9.1.4 NSP Post-Upscale Steps

This procedure describes different steps to be followed after upscale procedure.

1. Configure hosts and aliases on IXP/EFS/RSP

a) Open a terminal window and log in on any server in the IXP subsystem or EFS as `root`. b) Update the `/root/bulkconfig` file with the new NSP IP addresses.

c) Adjust the IXP subsystem/EFS. As `root` run:

```
# bc_adjust_subsystem.sh
```

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

2. Configure hosts and aliases on xMF

a) Refer to Update NSP IP adresses in the xMFs for TPD 3.X or Update NSP IP adresses in the xMFs for TPD 4.Xaccordingly to xMF platfrm version.

3. Configure the NSP application server's IP address.

a) Run the setAppServer script. As `root` run:

```
# /usr/TKLC/TKLCmf/bin/setAppServer
```

You'll be prompted:

```
Please enter an IP address for appserver:
```

b) Enter IP address of the NSP Primary WebLogic server and press <enter>. You'll be prompted:

```
XX.XX.XX.XX          appserver
Old appserver entry not found.  Adding
RCS_VERSION=1.X
Updating
hosts.byname...
Updating
hosts.byaddr...
Does the system have a 2nd Application Server (y or n) ?
```

c) Type y and press <enter>.

```
Please enter an IP address for appserver2:
```

Now enter the IP address the NSP Secondary WebLogic server

```
Updating hosts.byname...
Pushing hosts.byname map to blue-1b
... Updating hosts.byaddr...
Pushing hosts.byaddr map to blue-1b ...
#
```

4. Install Apache certificates

a) Configure Apache HTTPS Certificate (Optional)

5. Update A-Node IP address

a) Login into the NSP Oracle Box as oracle user and execute the following command. As oracle run:

```
$ sqlplus nsp/nsp
```

b) The SQL> prompt should appear.

In the SQL shell run the following SQL command to update the IP address (< IP of Primary WL > should be replaced with the new IP address of the Primary Weblogic)

```
SQL> UPDATE COR_SYSTEM_CONFIG SET CONFIGURATION_VALUE = '
nsp_primary_weblogic
 ' WHERE CONFIGURATION_NAME = 'ANODE.IP' ;
```

c) You should expect the following output:

```
1 row
updated. SQL>
```

d) Commit the changes and exit the SQL shell:

```
SQL> commit ;
SQL> exit ;
```

6. Check NSP Oracle server configuration

a) Check the server time and timezone.

7. Restart NTP service on all the NSP Four-Box servers

a) Login as root user on each server from NSP Four-Box setup. As root run:

```
# service ntpd restart
```

9.1.5 NSP Post-Upscale Sanity Test

This procedure describes different steps to be followed for the Post-Upscale Sanity tests.

1. **WebLogic Console**

   a) From Internet Explorer, connect to the WebLogic console using the following URL: *http://192.168.1.1:8001/console*

   Where `192.168.1.1` is the IP address of the WebLogic Primary

   Server. b) Login with user "weblogic"

2. **Health Check**

   a) Under the "**Environment**" heading, click on the "**Servers**" link

   b) The console would display the "**Summary of Servers**", with a list of the five servers, nsp1a, nsp1b, nsp2a, nsp2b and nspadmin.

   c) Entries in the columns "**State**" and "**Health**" should be "**RUNNING**" and "**OK**" for all five servers.

3. **NSP GUI**

   a) From Internet Explorer, connect to the NSP Application GUI using the following URL:*http://192.168.1.2:8001/nsp*

   Where `192.168.1.2` is the IP address of the Apache

   Server. b) Login with user "tekelec"

4. **Build Verification**

   a) In the top frame, on mouse-over on the link '**Portal**', click on the '**About**' link that will be displayed.

   A pop-up window with the build information will be displayed. b)

   The build version should display "Portal 9.0-X.Y.Z".

   Where 9.0-X.Y.Z should be the new build number.

9.1.6 Change Customer Icon

This procedure is optional and describes different steps to be followed for the updating the company Logo in place of standard Tekelec Logo.

1. **Copy Customer Icon File**

   a) Login as **tekelec** user on the NSP Server or Apache server in case of four box setup.

   b) A customer icon file shall be copied into the following directory /`opt/www/resources`/.

   You can place this icon by downloading, transferring via portable drives, etc.

2. **Verify Customer Logo Properties**

   a) The file must be named exactly as `customer_icon.jpg` and must belong to user **tekelec** in group **tekelec**.

   b) The **compression format** must be **Jpeg**, and **optimum width/height ratio** is **1.25**.

You can put any image you want; the suggested **minimum width/height** is **150** pixels..

9.1.7 Update NSP IP adresses in the xMFs for TPD 3.X

This procedure describes the steps to update the NSP IP addresses on XMF subsystems . This procedure is applicable to the all XMF subsystems.

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.
Note: This step is run on all servers in the subsystem and on standalone server.

1. Configure the NSP application server's IP address.

a) Log in as `root` on the 1A (or 0A in case of standalone) server.

b) Run setAppServer script

```
# /usr/TKLC/TKLCmf/bin/setAppServer

Please enter an IP address for appserver:
```

c) Enter IP address of the weblogic primary server

Output should be similar to below(if there is only "Does the system have a 2nd Application Server (y or n) ? " it is correct too):

```
XX.XX.XX.XX          appserver

Old appserver entry not
found.  Adding
RCS_VERSION=1.X
Updating
hosts.byname...
Updating
hosts.byaddr...
Does the system have a 2nd Application Server (y or n) ?
```

d) For set the ip of the weblogic secondary server answer **y** otherwise **n.** If you do not want to set weblogic secondary server answer **n:**

```
#
```

If you want to set weblogic secondary server answer **y**:

```
Please enter an IP address for appserver2:
```

Enter IP address of the weblogic secondary server

```
Updating hosts.byname...
Pushing hosts.byname map to blue-1b
... Updating hosts.byaddr...
Pushing hosts.byaddr map to blue-1b ...
#
```

e) Verify weblogic server entry is valid.

Note: Skip this step for PMF standalone server.

```
# ypcat hosts | grep appserver
```

For 1 weblogic server ouput should be similar to:

```
XX.XX.XX.XX         appserver NSPproAlarmServer
```

For 2 weblogic servers ouput should be similar to:

```
XX.XX.XX.XX         appserver NSPproAlarmServer
XX.XX.XX.XX         appserver2 NSPproAlarmServer2
#
```

f) Reboot the server

Note: The reboot may take up to 15 minutes while the MRV (Tekserver 1 systems only), and/or
Switches are being updated.

g) Reboot the rest of the servers in the subsystem.

h) Login to non-1A servers and verify weblogic server entry is valid

Note: Skip this step for PMF standalone server.

```
# ypcat hosts | grep appserver
```

For 1 weblogic server ouput should be similar to:

```
XX.XX.XX.XX         appserver NSPproAlarmServer
```

For 2 weblogic servers ouput should be similar to:

```
XX.XX.XX.XX         appserver NSPproAlarmServer
XX.XX.XX.XX         appserver2 NSPproAlarmServer2
#
```

2. Discover xMF Applications

a) From supported browser login to the NSP Application GUI as privileged user

b) Go to the Centralized Configuration

c) Navigate to **Equipment Registry Perspective** in left tree

panel. d) Navigate to the subsystem.

e) Select the XMF subsystem to synchronize by clicking on **XMF** under the correct Site

name. f) This will list the subsystem in the table

g) Click the **Synchronize** action in the table row for the XMF subsystem.

Note: This action includes both Application synchronization and Network Element synchronization

9.1.8 Update NSP IP adresses in the xMFs for TPD 4.X

This procedure describes the steps to update the NSP IP addresses on XMF subsystems . This procedure is applicable to the all XMF subsystems.

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.

1. Configure the NSP application server's IP address.

Note: This step is run on all servers in the subsystem and on standalone

server. a) Log in as `root` on the server.

b) Run setAppServer script

```
# /usr/TKLC/TKLCmf/bin/setAppServer
```

```
Please enter an IP address for appserver:
```

c) Enter IP address of the weblogic primary server

Output should be similar to below(if there is only "Does the system have a 2nd Application Server (y or n) ? " it is correct too):

```
XX.XX.XX.XX          appserver

Old appserver entry not found.  Adding
RCS_VERSION=1.X
Updating hosts.byname...
Updating hosts.byaddr...
```

```
Does the system have a 2nd Application Server (y or n) ?
```

d) For set the ip of the weblogic secondary server answer **y** otherwise **n.** If you do not want to set weblogic secondary server answer **n:**

```
#
```

If you want to set weblogic secondary server answer **y**:

```
Please enter an IP address for appserver2:
```

Enter IP address of the weblogic secondary server

```
Updating hosts.byname...
Pushing hosts.byname map to blue-1b ...
Updating hosts.byaddr...
Pushing hosts.byaddr map to blue-1b ...
#
```

e) Reboot the server

2. Discover xMF Applications

Note: This step is run when previous step is done on all servers in the subsystem. a) From supported browser login to the NSP Application GUI as privileged user b) Go to the Centralized Configuration

c) Navigate to **Equipment Registry Perspective** in left tree panel. d) Navigate to the subsystem.

e) Select the XMF subsystem to synchronize by clicking on **XMF** under the correct Site name. f) This will list the subsystem in the table

g) Click the **Synchronize** action in the table row for the XMF subsystem.

Note: This action includes both Application synchronization and Network Element synchronization

9.1.9 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 assume 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.

Update bulkconfig and adjust the subsystem/EFS.

a) Open a terminal window and log in on any server in the IXP subsystem or EFS as `root`. b) Update the `/root/bulkconfig` file with the new NSP IP addresses.

c) Adjust the IXP subsystem/EFS. As `root` run:

```
# bc_adjust_subsystem.sh
```

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

9.2 NSP Upscale Backout Procedure

This procedure describes how to backout the NSP One-Box to NSP Four-Box upscale.

Note: No further upscale is allowed after this procedure is executed. Upscale procedure need to be started again from scratch starting with operation system installation.

1. **NSP Upscale Backout**

   a) Login as `root` user on the NSP Oracle server (Four-Box, originally NSP One-Box). Enter the platcfg menu. As `root` run:

   ```
   # su - platcfg
   ```

   b) Navigate to **NSP Configuration ⊙ Upscale Backout** and press `<enter>`.

2. **Install A-Node on NSP One-Box server (NSP Oracle server in Four-Box)**

   a) Login as `root` to the NSP One-Box b) Insert the XMF CD to the cdrom

   c) If ISO is available copy the iso to NSP server at some location. d) Execute as root user the following command.

   As `root` run:

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

   When asked for ISO, provide the complete ISO path (e.g. `/var/TKLC/upgrade/`*`xmf_iso_filename`*)

   e) Type `yes` and press `<enter>` to confirm the installation.

   f) No reboot needed

3. **Restart the NTP service**

   a) Login as `root` user on the NSP One-Box server. As `root` run:

   ```
   # service ntpd restart
   ```

9.3 NSP Backup Procedures

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

9.3.1 Automatic Backup

9.3.1.1 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). b) As `root` run:

   ```
   # crontab –l
   ```

   c) If the output of the previous step is:

```
no crontab for root
```

Then no crontab is activated for `root`. Continue with the next step to activate the backup. Example of activated backup:

```
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.

2. Activate backup

Note: Execute this step only if backup is not

activated. a) As `root` run:

```
# 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.

Example directory name:

```
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

9.3.1.2 Deactivate Automatic NSP Backup

This procedure describes how to deactivate automatic NSP backup.

Deactivate backup

a) Login as `root` on NSP One-Box or NSP Primary WebLogic server (Four-Box). b) View the contents of the crontab for root.

As `root` run:

```
# 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. As `root` run:

```
# 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
```

9.3.1.3 Change Automatic NSP Backup Time and Location

Execute this procedure to change an automatic backup time or location

1. Change the backup time

a) Login as the `root` user on NSP One-Box server or NSP Primary WebLogic server (Fou-Box)
b) List the content of the crontab file. As `root` run:

```
# crontab –l
```

Locate the line with a record `LaunchExpNSPdp.sh` for NSP automatic backup.

c) Edit the crontab file. As `root` run:

```
# crontab –e
```

Replace the values of backup time with new values of backup time.

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
```

d) A new crontab should be installed. List the content of the crontab file to verify changes. As `root`
run:

```
# crontab –l
```

e) The output will show the changed crontab entry.

2. Change the location of backup files

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

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

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

9.3.2 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.

NSP backup procedure

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

b) Execute below commands

Create a directory having write permission for the Oracle user

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

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

Note: 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:

1. Oracle connection string (NSP/NSP) must not be modified
2. Schema name to export (NSP) must not be modified
3. 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.

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

Login as a `oracle` user on NSP Server (In case of Onebox configuration) or NSP Oracle server
(In case of Four box configuration)

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

As `oracle` run:

```
# 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 a external source.

9.3.3 Realm Backup

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

Take realm backup

a) Login as `root` user on NSP One-Box or NSP Primary WebLogic server (Four-Box) or NSP Guest (DIH Setup).

b) 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.sh
 /opt/nsp/scripts
# mkdir /opt/nsp/realmbackup
# ./LaunchExpNSPrealm.sh /opt/nsp/realmbackup
```

c) 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`

9.3.4 System Files Backup

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

Backup system files

a) Login as `root` user on NSP One-Box or any NSP server in case of Four-Box configuration. b) 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 saved in that box itself. Copy these files to an external source.

9.4 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

Start NSP service

a) Open a terminal window and log in as `tekelec` user on NSP Primary WebLogic server
b) Execute following command to start NSP service.

As `tekelec` run:

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

9.5 Start NSP Service on Secondary when Primary Is Down

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

Start NSP service

a) Open a terminal window and log in as `tekelec` user on NSP Secondary WebLogic server b) Execute following command to start NSP service.

As `tekelec` run:

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

9.6 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. Open a terminal window and log in as `root` on the NSP One-box or the Apache 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.

9.7 Copy NSP Backup

1. Copy NSP Backup

a) 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
```

1. It will ask for backup user password, enter the password for backup user and press **ENTER.**

2. **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).
3. */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*
4. To note exact path of the backup you can use steps mentioned in step 2 below.
5. *local_backup_dir* should be replaced by a directory name of the Customer choosing.
6. After successful completion of the command the backup should be available at the *local_backup_dir* folder.
7. 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 `tekelec` user on the NSP Server (or NSP Oracle server in case of 4-box configuration). 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 will 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
25th July 2011

10 xMF Maintenance Procedures

10.1 xMF Reset Switch to Factory Defaults

This procedure configures a switch back to factory defaults. This procedure can be used for any switch location or color.

Repeat for all switches you need to set to defaults.

Note: In case in the procedure would failed, refer to 909-2247-01 PIC 9.0 Maintenance guide in order to recover the switch from rommon prompt.

A. Configure and access the serial console from the server on the switch
    a. Refer to Customer integration manual 909-2241-01 section 14.1.1
B. Reset the switch to factory default
    a. If you are reconfiguring a switch backup the current config in a file using the command

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

    b. Refer to Customer integration manual 909-2241-01 section 14.1.3 or 14.1.5 to reset the switch depending on your model

10.2 Frame Switch Configuration

10.2.1 For PIC 9.0.1 and lower

This procedure provides instructions to perform configuration of the Cisco switches for (Tekserver and HP frames).

Note: For TEKIII/DL380G6, configure only switch yellow-sw1-1 from XMF-1A server, as a TEKIII/DL380G6 can only configure one switch at a time.

a) Log onto XMF-1A as root.

Note: FOR T1000 AND T1100 - DO NOT RUN THIS PROCEDURE OTHER THAN XMF-1A.

Note: For TEKIII/DL380G6 only:

Log onto XMF-1B to configure switch blue-sw1-1.

Log onto XMF-1C to configure switch Yellow-sw2-1.

Log onto XMF-1D to configure switch blue-sw2-1.

Log onto XMF-1E to configure switch Yellow-sw3-1.

Log onto XMF-1F to configure switch blue-sw3-1.

b) If you are configuring a 2950 switch you must first update the FRAME_SWITCH variable. And run the vlan configuration script.

Note: This step is only for the 2950 switch, for 4948 switch proceed to next step.

Edit the TKLCplat profile:

```
#vim /etc/profile.d/TKLCplat_conf.sh
```

Update “FRAME_SWITCH” to “2950”:

```
export FRAME_SWITCH=2950
```

Save and exit.

c) Run the vlan configuration script:

```
#cd /usr/TKLC/plat/etc
#vlanconf_setup.sh > vlan.conf
```

d) Run xmfconfig script to configure all switches:

Note: This step is for both 2950 and 4948 switches.

```
#/usr/TKLC/plat/bin/xmfconfig
```

e) Select what you want to configure:

```
| - xMF Configuration Utility Initial
| Configure Switches -> Select 1
| [E]xit
Selection ->
```

Select **1** and press **<enter>** to confirm. If you want to exit, press **E** and press **<enter>**.

```
Selecting Switch Configuration
How many switches to configure [1|2|4]?
```

Select **1**, **2** or **4** and press **<enter>** to confirm.

Note: This operation will take about 20+ minutes.

Note: During the switch config you may be prompted. Do not enter any value until you return back to the main xMF Configuration Utility menu. This process will also take less time on a Tek III due to only Tek III configures one switch at a time.

Note: TEK III/DL380G6 servers will not query for the number of switches as a TEK III/DL380G6 can only configure one switch at a time.

Note: If configuring TEK III/DL380G6, perform the xmfconfig for the yellow switch from the 1A server then perform the xmfconfig from the 1B server to configure the blue switch.

f) Verify that xmfconfig script was executed properly:

```
# less /var/TKLC/log/xMF/switchconfig.blue-sw1-1.log.%
# less /var/TKLC/log/xMF/switchconfig.yellow-sw1-1.log.%
```

where **%** is the date of file creation, like:

```
# less /var/TKLC/log/xMF/switchconfig.yellow-sw1-1.log.082307
```

Note: The blue-sw1-1.log will not exist on TEK III 1A server; it should exist on TEK III 1B server.

xmfconfig file should be additionally created in /usr/TKLC/plat/etc/ext.

```
# ls /usr/TKLC/plat/etc/ext
```

Expected output:

```
# xmfconfig
```

g) Logoff:

```
# exit
```

10.2.2 For PIC 9.0.2 and higher

This procedure is asuming the switch was reset to the default config as explained in the section 10.1.

Configure the switch using the appropriate template

a. Refer to Customer integration manual 909-2241-01 section 14.1 to select and the appropriate configuration template and adapt it to the customer IP network.
b. As there is no log file for the following steps it is recomanded to enable the log feature from your terminal in case something would not work as expected and assistance is required.
c. Move from the user mode to priviledge mode and than to config mode

```
Switch# enable
Switch# configure terminal
```

Note : if you reset the switch to factory default no password should be requested to connect on it and move to enable mode.

d. Paste all the commands from the template config you have adated to you network. The lines you need to customize are higlited with Yellow comments. You can paste the command in block and not necessary one by one but don't do it with too much commands at a time in order to take care if an error message would appear.
e. Once the config is in place you can check it is matching your expectation using the command

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

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

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

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

```
Switch# reload
```

h. Move from the user mode to priviledge mode and than to config mode

```
Switch# enable
Switch# configure terminal
```

i. Finally to configure the SSH access to the switch refer to Customer integration manual 909-2241-01 section 14.1.7
j. Once the config is in place you can check it is matching your expectation using the command

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

k. If the configuration is fine than you can save it in the flash in order to have it automatically reloaded if the switch reboot

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

l. If there is an issue in your config you can can reboot the switch without saving and than restart the config from the step a

10.3 Reset MRV to Factory Defaults

This procedure configures the MRV back to factory defaults.

1. Serially connect to MRV from Tekserver.

a) Login as root to 1A server
b) Serially connect to MRV

```
# minicom MRV-console
```

Note: Hit enter if no login prompt is displayed.

```
Welcome to minicom 2.00.0
OPTIONS: History Buffer, F-key Macros, Search History Buffer, I18n
```

```
Compiled on Jan 25 2003, 00:15:18. Press CTRL-A Z for help on special keys
```

c) Login as tklc or InReach

2. Enter enable mode and reboot MRV.

a) Enter enable mode by en and password

```
tklc:0 >en
Password: XXXX
```

b) Execute reload command to reboot MRV

```
tklc:0 >>reload
```

c) Type <y> to confirm

```
Do you really want to proceed? y/n y
```

Note: Watch for menu upon reboot, you only have 8 seconds to respond on this step. If you do not respond within the 8 seconds, the MRV will reboot.

d) Select **<L>** to login in System Setup and type password

```
Welcome to In-Reach ppciboot version 3.4.0.1
[B] Boot System
[L] Login in System Setup
L
Password: XXXX
```

e) Enter **<*>** to get to the menu to reset MRV to factory defaults.

```
Main Menu
[1] Boot from network:
[2] Save software image to flash
[3] Boot from flash:
[4] Time Out, in seconds (0=disabled):
[5] IP Configuration Menu
[6] Update Ppciboot Firmware
[7] Ethernet Network Link:
[8] Change PPCiBoot password
[*] Reset to System Defaults
[S] Save Configuration
[B] Boot System
Make a choice:
* <enter password if prompted>
```

f) Press the number **<1>** to reset the ppciboot configuration.

Note: Do not hit enter. You will automatically be taken back to the previous menu after this completes.

```
[1] Reset ppciboot configuration
[2] Reset Linux system configuration
[3] Reset ppciboot and Linux system configuration
Make a choice: 1
```

g) Enter **<*>** to get to the menu to reset MRV to factory defaults.

```
Main Menu
[1] Boot from network:
[2] Save software image to flash
[3] Boot from flash:
[4] Time Out, in seconds (0=disabled):
[5] IP Configuration Menu
[6] Update Ppciboot Firmware
```

```
[7] Ethernet Network Link:
[8] Change PPCiBoot password
[*] Reset to System Defaults
[S] Save Configuration
[B] Boot System
Make a choice:*
```

h) Press the number **<2>** to reset the ppciboot configuration.

Note: Do not hit enter. You will automatically be taken back to the previous menu after this completes

```
[1] Reset ppciboot configuration
[2] Reset Linux system configuration
[3] Reset ppciboot and Linux system configuration
Make a choice: 2
```

i) Enter **<b>** to reboot the MRV.

Allow MRV to boot. The MRV is set to factory defaults.

j) After loading to factory defaults enter **<n>** and hit <enter>

```
This unit has loaded to factory defaults, would you like to
run Initial Connectivity Setup?(y/n):
```

k) Press **<ctrl>+<a>** to show menu and press **<q>** to disconnect from MRV

l) Select **yes** and **<enter>** to leave without reset

10.4 Enable Redundant Wan on IMF

This procedure provides instructions to enable redundant wan on IMF.

Note: Run this procedure only on T1000 and T1100.

Enable redundant wan

a) Login to server as root

b) Add following line to the script `/etc/profile.d/TKLCplat_conf.sh`:

```
export REDUNDANT_WAN=yes
```

c) Execute export command:

```
# export REDUNDANT_WAN=yes
```

d) Make sure that you have properly connected cables to switch according to the xMF Switch Config.

10.5 Start xmfsingle.pl for single server single switch configuration

This procedure is used during a single switch configuration existing with a single server for PIC 9.0.1 and lower.
For PIC 9.0.2 and higher use the default or alternate configuration template from the Customer integration manual 909-2241-01 section 14.1.

Run xmfsingle.pl script

a) Login to server as root

b) For single server single switch configuration run xmfsingle.pl:

```
# xmfsingle.pl
```

c) Verify that xmfsingle.pl script was executed properly

If switch configuration was successful this message will display:

```
Switch yellow-sw1-1 successfully configured.
```

10.6 Custom Layer 2/3 switch confguration

This procedure is used to configure a vrrp custom switch configuration for PIC 9.0.1 and lower.
For PIC 9.0.2 and higher use the default or alternate configuration template from the Customer integration manual 909-2241-01 section 14.1.

1. xmfLayerThree.pl configuration file

a) Login to server as root

b) The custom settings of the switch's configuration file will reside in a file called `/usr/TKLC/plat/etc/xmfLayerThree.csv`

This file must be edited with the appropriate setting. This file includes the custom setting for the yellow and blue switch.

2. xmfLayerThree.csv template

a) The xmfLayerThree custom config file is written in the CSV format.

Each line begins with a keyword indicating the yellow or blue switch that the line holds. The keyword is mandatory. Each line must begin with the keyword. Then the rest of the line contains various values. Keywords and values are separated with comma. There are no white spaces on the line.

```
yelvrrp,<customer_vlan>,<IP_address>,<mask>,<network_gateway>,<vrrp_priority>
,<layer3_vlan>,<IP_address>,<mask>,<network_gateway>,<vrrp_priority>
bluvrrp,<customer_vlan>,<IP_address>,<mask>,<network_gateway>,<vrrp_priority>
,<layer3_vlan>,<IP_address>,<mask>,<network_gateway>,<vrrp_priority>
```

3. xmfLayerThree.csv example

a) We need to create the `xmfLayerThree.csv` file for the following subsystem:

Customer vlan ID: Vlan200

Customer vlan IP: 192.168.253.5

Customer vlan mask: 255.255.255.0

Customer vlan gateway: 192.168.253.1

Customer vlan interface priority: 2

VRRP vlan ID: Vlan30

VRRP vlan IP: 10.240.10.2

VRRP vlan mask: 255.255.255.0

VRRP vlan gateway: 10.240.10.1

VRRP vlan interface priority: 10

Above are the setting for the yellow switch, blue switch settings are similar as indicated below. Do not edit the yelvrrp or bluvrrp fields as these are needed for the scipt to work properly, they indicate the yellow and blue configurations respectively.

Then the corresponding xmfLayerThree.csv file looks like:

```
$ cat xmfLayerThree.csv
yelvrrp,Vlan200,192.168.253.5,255.255.255.0,192.168.253.1,2,Vlan30,10.240.10
.2,255.255.255.0,10.240.10.1,10
bluvrrp,Vlan200,192.168.253.6,255.255.255.0,192.168.253.1,2,Vlan30,10.240.10
.3,255.255.255.0,10.240.10.1,10
```

4. Run xmfLayerThree.pl

a) Edit the xmfLayerThree.csv file with the desired settings.

Note: Do this for on both 1A and 1B servers.

```
#vim /usr/TKLC/plat/etc/xmfLayerThree.csv
```

b) Run xmfLayerThree.pl

Note: Run this step for 1A and 1B

servers. xmfLayerThree.pl has two

options:

The first option is to run xmfLayerThree.pl with no arguments. This only creates the custom switch configuration files. This allows for a review of the configuration file before applying them to the switch. The configuration files are:

`/usr/TKLC/plat/etc/4948-IMF-yellow-sw1-1.layer3`

`/usr/TKLC/plat/etc/4948-IMF-blue-sw1-1.layer3`

Run the command as follows:

- The first option is to run xmfLayerThree.pl with no arguments. This only creates the custom switch configuration files. This allows for a review of the configuration file before applying them to the switch. The configuration files are:

  `/usr/TKLC/plat/etc/4948-IMF-yellow-sw1-1.layer3`

  `/usr/TKLC/plat/etc/4948-IMF-blue-sw1-1.layer3`

  Run the command as follows:

  ```
  # xmfLayerThree
  ```

- The second option is to run xmfLayerThree.pl with -c argrument. With this argument passed the custom switch configuration files will be created and immediately applied to the corresponding switch.

  ```
  # xmfLayerThree -c
  ```

5. **Verify that xmfLayerThree.pl script was executed properly**

If switch configuration was successful this message will display:

```
# less /var/TKLC/log/xMF/switchconfig.yellow-sw1-1.log.%
# less /var/TKLC/log/xMF/switchconfig.blue-sw1-1.log.%
```

10.7 Temporary xMF customer IP assignment

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

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

Configure Vlan tagging and assign ip address

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

b) Execute following commands:

```
# modprobe 8021q
# vconfig add <CUST ITF> 200
# ifconfig <CUST ITF>.200 <CUST IP ADDRESS> netmask <MASK>
# route add default gw <DEFAULT ROUTE IP ADDRESS>
```

Remark: The `<CUST ITF>` is to replace by eth01 for HP and T1200 servers, by eth91 for T1100 servers and by eth81 for T1000.

c) Transfer Application ISO on the server

d) Once ISO file is transferred **reboot** the server.

```
# reboot
```

10.8 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
```

11 IXP Maintenance Procedures

11.1 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.

11.2 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

a) 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

a) 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
```

11.3 Convert feeds in backward compatible mode

a) Open a terminal window and log in as `tekelec` user on the NSPOne-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
```

11.4 Configure Sessions for Legacy the 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.
d) 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.

11.5 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.

11.6 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.

11.7 Set Behavior Mode for IXP xDR Storage Server

This procedure describes how to set the behavior mode for a specific IXP xDR Storage Server that is part of the IXP xDR storage pool.

Set IXP xDR Storage server behavior mode

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**.

11.8 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.

Turn the MSA back on

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.

11.9 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.

11.10 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 xDR Storage Server
- IXP PDU Storage Server
- IXP Standard Export Server.

Prerequisite: This procedure assume 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. Increase the maximum size of the UNDO tablespace.

Note: This step is applicable to IXP xDR Storage running Oracle 10g with 12 disks only. Performance issues has been discovered with Oracle 10g running on PIC 9.0 release when the UNDO tablespace is 8GB size. This step will increase the UNDO tablespace to 16GB.

a) Open a terminal window and log in on IXP xDR Storage server server running Oracle 10g you are about to add to the IXP subsystem as `oracle` .

b) Verify Oracle version. As `oracle` run: As `root` run:

```
$ sqlplus / as sysdba
```

If the SQL*Plus banner reads the following, DO NOT run this procedure:

```
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 – Production
```

If the SQL*Plus banner reads similar to the following:

```
Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.x.0 - Production
```

proceed to the next step.

c) Verify current size of UNDO tablespace. Run:

```
SQL> set linesize 150
SQL> column file_name format a40
SQL> select FILE_NAME,MAXBYTES from dba_data_files where TABLESPACE_NAME =
'UNDO' order by 1;
```

If the maximum size of the UNDO tablespace is currently 8GB, the output will be as follows:

```
FILE_NAME                                 MAXBYTES
---------------------------------------- ----------
/opt/oracle/oradata/IXP/undo01.dbf       2147483648
/opt/oracle/oradata/IXP/undo02.dbf       2147483648
/opt/oracle/oradata/IXP/undo03.dbf       2147483648
/opt/oracle/oradata/IXP/undo04.dbf       2147483648
```

If so, please proceed to the next substep. If the maximum size of the UNDO tablespace is already
16GB, the output will be as follows and you DO NOT need to run the rest of this step:

```
FILE_NAME                                  MAXBYTES
------------------------------------------ ----------
/opt/oracle/oradata/IXP/undo01.dbf       4294967296
/opt/oracle/oradata/IXP/undo02.dbf       4294967296
/opt/oracle/oradata/IXP/undo03.dbf       4294967296
/opt/oracle/oradata/IXP/undo04.dbf       4294967296
```

proceed to the next step.

d) Update the maximum size of UNDO tablespace to 16GB. Run:

```
SQL> ALTER DATABASE DATAFILE '/opt/oracle/oradata/IXP/undo01.dbf'
AUTOEXTEND ON MAXSIZE 4G;
SQL> ALTER DATABASE DATAFILE '/opt/oracle/oradata/IXP/undo02.dbf'
AUTOEXTEND ON MAXSIZE 4G;
SQL> ALTER DATABASE DATAFILE '/opt/oracle/oradata/IXP/undo03.dbf'
AUTOEXTEND ON MAXSIZE 4G;
SQL> ALTER DATABASE DATAFILE '/opt/oracle/oradata/IXP/undo04.dbf'
AUTOEXTEND ON MAXSIZE 4G;
```

The result of all commands above should be:

```
Database altered
```

e) Verify UNDO tablespace maximum of 16GB. Run:

```
SQL>  select FILE_NAME,MAXBYTES from dba_data_files where TABLESPACE_NAME =
'UNDO' order by 1;
```

If the maximum size of theUNDO tablespace is now 16GB, the output will be as follows:

```
FILE_NAME                                  MAXBYTES
------------------------------------------ ----------
/opt/oracle/oradata/IXP/undo01.dbf       4294967296
/opt/oracle/oradata/IXP/undo02.dbf       4294967296
/opt/oracle/oradata/IXP/undo03.dbf       4294967296
/opt/oracle/oradata/IXP/undo04.dbf       4294967296
```

Exit Oracle commandline:

```
SQL> exit
```

2. 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 editted the `/etc/hosts` file any time before (which 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.

- If your server is configured with the default IPs from manufacturing and other subsystem IPs are not accessible run 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
     ```

- If the server has already been configured with the customer IPs during the manufacturing installation and all the servers in the subsystem are already reachable run the following steps:

  1. 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
```

3. 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.

a) 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. 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.**

5. 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.

6. 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.

7. Send an email with a request to receive the license key file

Copy the `IxpSubsystemKey.data` file to a machine with an email access; then, send the file, along with a copy of the purchase order where the license part numbers are mentioned, to the following address: `cssg.product.license.request@tekelec.com`

8. Transfer the license file to the IXP Active Master server

a) Open a terminal window and log in as `cfguser` on the IXP Active Master server.
b) Copy the `IxpLicenseKey.data` file to the IXP Active Master server to `/home/cfguser/` directory.

9. Activate license

As soon as the file has been detected and verified, the existing temporary license alarm(s), if any, is automatically cleared.

10. 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.

11.11 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.

11.12 Remove Server from the IXP Subsystem

This procedure describes how to remove the IXP server from the IXP subsystem.

Note: Do not remove 1A server from the subsystem. This operation is not supported.

1. **Offload the IXP server**
   a) 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**
   a) 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:
   ```
   # shutdown -h
   ```

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

f) Open a web browser and log in NSP application interface.
g) Click on **Centralized Configuration**.
h) Navigate to **Mediation ⊙ Sites ⊙ IXP Site ⊙ IXP ⊙ IXP subsystem ⊙ Servers**.
i) In the list of the servers displayed on the right side mark the server that you want to remove.
j) Click on **Delete**.
k) Right click on IXP subsystem and press **Apply changes.**
l) 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
```

11.13 Installation of External Datawarehouse

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

- Oracle 10g/11g must be installed
- 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

As `oracle` (xDR Storage server) or `cfguser` (any other IXP server) run:

```
$ /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 exists 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. 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**.** 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) 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. 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. Install package, procedures and tables for the External DatawareHouse / Oracle feeds feature

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

a) 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 exists and cannot be deleted).

b) Optionally, install and enable nightly jobs. Check with the DBA before activating these jobs. 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.

11.14 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.

a) Create user `cfguser` and group `cfg`

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

2. Create export directories

Note: Run this step on customer provided server

a) 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 this directories is `cfguser` and group `cfg`.

3. Update the `/etc/exports` file

Note: Run this step on customer provided server

a) 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.

a) 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.

a) 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)

a) 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_?/.

12 Report Server Platform Maintenance Procedures

12.1 Uninstall Report Server Platform

This procedure describes how to install the Report Server Platform software from Report Server..

Uninstall Report Server package

a) Log in as `root` on the Report Server.

b) Uninstall Report Server software. As `root` run:

```
# /var/TKLC/rsp/uninstall.sh
```

you will see the following prompt:

```
############################################################
#       Uninstalling Report Server Platform 7.1.0-16.1.0
############################################################
REPORT_SERVER_DESIGI=PRIMARY
You are about to uninstall Primary Report Server.
Are you sure? [y/n]:
```

type `y` and press `<enter>` to confirm this operation.

c) Get TKLCrsp rpm package information.

As `root` run:

```
# rpm -qa TKLCrsp
```

Note down the exact name of installed TKLCrsp package. Uninstall this package. As `root` run:

```
# rpm -qe TKLCrsp-9.0.0-64.2.0.i386
```

where you need to replace *9.0.0-64.2.0.i386* with the exact installed version you received in previous step.

d) Remove the RSP

directories. As `root` run:

```
# rm -rf /var/TKLC/rsp
# rm -rf /var/TKLC/boe_inst_cds_31
```

e) Remove the following file.

As `root` run:

```
# rm /usr/TKLC/plat/etc/tnsnames.d/rsp.tns
```

f) Remove RSP related records from tnsnames.ora

file. As `root` run:

```
# vi /usr/lib/oracle/10.2.0.3/client/network/admin/tnsnames.ora
```

Remove RSP related records. Leave IXP and NSP tnsname records

untouched. g) Using platcfg menu remove the following aliases from

`/etc/hosts` file:

- `cms_db_server`
- `boe_cms`
- any alias ended with `rds_db_server`

13 Plateform based Maintenance Procedures

13.1 PM&C Disaster Recovery

This document does not cover PM&C application that is part of the HP C-Class Blade system. For PM&C Disaster Recovery procedure follow document 909-1638-001 revision 1.3 and more for the PM&C Disaster Recovery procedure.

13.2 Install Operating System on xMF G5 Rackmount Servers

This procedure describes how to install the operating system on the HP DL380 and ML350 G5 rackmount servers.

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 G5 servers.

1. Power on and enter the BIOS

a) Power on the external disk arrays.
b) Power on the server.
Within a couple of seconds, the `F9 Setup` message appears in the bottom-right corner.
c) Press **F9**.
The message changes to `F9 Pressed`.

2. Set up the BIOS date and time

a) Select the Main menu and set the System Date and System Time values to Greenwich Mean Time (GMT).
b) Insert the TPD DVD/CD.
c) Save the changes and exit the BIOS.
The system boots to the TPD installation screen.

3. Install the operating system

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

- For the serial console, enter:

```
boot: TPDnoraid console=ttyS0
```

- For the iLO or VGA/keyboard, enter:

```
boot: TPDnoraid console=tty0
```

4. Reboot the 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.

13.3 Install Operating System on xMF G6 Rackmount Servers

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

For an estimated time for this procedure, refer to the applicable flowcharts in MF Server Disaster Recovery T1100, T1200, G5 , G6.

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.

1. Power on and enter the BIOS

a) Power on the external disk arrays.
b) Power on the server.
Within a couple of seconds, the `F9 Setup` message appears in the bottom-right corner. c) Press **F9**.
The message changes to `F9 Pressed`.

2. Set up the BIOS iLO

Note: The serial ports on HP DL360 and DL380 G6 rackmount servers need to be configured so that the serial port used by the BIOS and TPD are connected to the iLO Virtual Serial Port (VSP). This allows the remote administration of the servers without the need for external terminal servers. If this configuration has not been completed correctly and the server is rebooted, then the syscheck test (`syscheck -v hardware serial`) will fail.

a) Select **System Options ⊙ Serial Port Options**. b) Change the following settings:

- **Embedded Serial Port** to **COM2**
- **Virtual Serial Port** to **COM1**

c) Save the changes and exit the BIOS.
The system boots to the TPD installation screen.

3. Disable Hyper-threading (only PMF)

Note: This step is applicable only for PMF.

a) Reboot the server.
b) As the computer boots, press **F9** to access the BIOS setup utility and press **Enter**.
c) Select **System Options** and press **Enter**.
d) Select **Processor Options** and press **Enter**.
e) Select **Intel Hyper threading Options** and press **Enter**.
f) Select **Disable** and press **Enter**.
g) Press **Esc** to exit the utility.
h) Press **F10** to confirm the exit from the utility.

4. Set up the BIOS date and time

a) Select the **Main** menu and set the **System Date** and **System Time** values to Greenwich Mean Time (GMT).
b) Insert the TPD DVD/CD.

5. Install the operating system

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

- For the serial console, enter:

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

- For the iLO or VGA/keyboard, enter:

```
boot: TPDnoraid console=tty0 diskconfig=HPHW,force
```

6. Reboot the 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.

13.4 Install Operating System on T1200 Server

This procedure describes how to install the operating system on the T1200 server.

Before you perform this procedure, make sure that you have the appropriate Tekelec Platform Distribution (TPD) DVD/CD or ISO file available.

1. Power on and enter the BIOS

a) Power on the server.
Within a couple of seconds, the `Press F2` message appears. b) Press **F2** to enter the BIOS setup screen.

2. Set up the BIOS date and time

a) Select the **Main** menu and set the **System Date** and **System Time** values to Greenwich Mean Time (GMT).
b) Insert the TPD DVD/CD.
c) Save the changes and exit the BIOS.
The system boots to the TPD installation screen.

3. Install the operating system

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

- For the Remote Management Module (RMM) console, enter:

```
boot: TPD console=tty0
```

- For the Intelligent Platform Management Interface (IPMI) Serial-Over-LAN (ISOL) console (serial connection), enter:

```
boot: TPD
```

4. Reboot the 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.

13.5 Install Operating System on T1100 Server

This procedure describes how to install the operating system on the T1100 server. Before you perform this procedure, make sure that you have the appropriate Tekelec Platform Distribution (TPD) DVD/CD or ISO file available.

1. Power on and enter the BIOS

a) Power on the server.
Within a couple of seconds, the `Press F2` message appears. b) Press **F2** to enter the BIOS setup screen.

2. Set up the BIOS date and time

a) Select the **Main** menu and set the **System Date** and **System Time** values to Greenwich Mean Time (GMT).
b) Insert the TPD DVD/CD.
c) Save the changes and exit the BIOS.
The system boots to the TPD installation screen.

3. Install the operating system

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

- For install directly on server (VGA/keyboard), enter:

```
boot: TPD console=tty0
```

- For the remote control (MRV or OOBM), enter:

```
boot: TPD
```

4. Reboot the 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.

13.6 Install Operating System on G5 Rackmount Servers

This procedure describes how to install the operating system on HP G5 rackmount servers.

1. Date and Time setup

a) Power on the server.
b) Power on disk arrays if they are connected.
c) Wait until the server will boot to the following message:

```
Press "F9" key for ROM-based Setup Utility
Press "F10" key for System Maintenance Menu
Press "F12" key for PXE boot
```

d) Press `<F9>` to enter **ROM-Based Setup Utility**
e) Navigate to **Date and time**
f) Set actual date end time
g) Press `<ENTER>`
h) Insert TPD CD into drive

i) Leave setup utility

2. Enter Installation Mode

a) Let system boot into TPD installation screen.
b) Enter installation parameters:

- If the external storage disk array is attached to server enter:

  For serial console:

  ```
  boot: TPDnoraid drives=cciss/c1d0 console=ttyS0
  ```

  For VGA/keyboar and iLO:

  ```
  boot: TPDnoraid drives=cciss/c1d0 console=tty0
  ```

- If the extarnal storage disk array is not attached to server enter:

  For serial console:

  ```
  boot: TPDnoraid console=ttyS0
  ```

  For VGA/keyboard and iLO:

  ```
  boot: TPDnoraid console=tty0
  ```

c) The installation process will display the progress of the system and packages installation.
d) At the end of installation the CD will be ejected from CD-ROM drive.
Remove the CD from tray and press `<ENTER>` to reboot the server.

13.7 Install Operating System on G6 Rackmount Servers

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

Before you perform this procedure, make sure that you have the appropriate TPD DVD/CD or ISO file available.

1. Power on and enter the BIOS

a) Power on the external disk arrays.
b) Power on the server.
Within a couple of seconds, the `F9 Setup` message appears in the bottom-right corner. c) Press **F9**.
The message changes to `F9 Pressed`.

2. Set up the BIOS date and time

a) Select the **Main** menu and set the **System Date** and **System Time** values to Greenwich Mean Time (GMT).
b) Insert the TPD DVD/CD.

3. Set up the BIOS iLO

Note: The serial ports on HP DL360 and DL380 G6 rackmount servers need to be configured so that the serial port used by the BIOS and TPD are connected to the iLO Virtual Serial Port (VSP). This allows the remote administration of the servers without the need for external terminal servers. If this configuration has not been completed correctly and the server is rebooted, then the syscheck test (`syscheck -v hardware serial`) will fail.

a) Select **System Options ⊙ Serial Port Options**. b) Change the following settings:

- **Embedded Serial Port** to **COM2**
- **Virtual Serial Port** to **COM1**

c) Save the changes and exit the BIOS.

The system boots to the TPD installation screen.

4. **Install the operating system**

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

- For the serial console, enter:

```
boot: TPDnoraid console=ttyS0 diskconfig=HPG6,force
```

- For the iLO or VGA/keyboard, enter:

```
boot: TPDnoraid console=tty0 diskconfig=HPG6,force
```

5. **Reboot the 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.

13.8 Install Operating System on Gen8 Rackmount Servers

Refer to 909-2240-01 PIC 9.0 Manufacturing Installation Procedure section 3.1 HP Gen8 Rackmount Platform

13.9 IPM Blade Servers Using PM&C Application

Refer to 909-2209-001 Platform 6.x Configuration Procedure Reference section 3.8.10 IPM Servers Using PM&C Application

14 External Software Configuration

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

3. Auto resize popup windows

On windows workstations

a) On windows workstations 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

Note: This setting needs to be done for IE7 only.

a) On windows workstations 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) On windows workstations 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) On windows workstations navigate to **Tools ⊙ Internet Options**

b) Select **Security** tab

c) Select **Internet** zone

d) Click on the **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

Go to **Tools ⊙ Internet Options**. Select the **Advanced** tab. In the **Browsing** section set to **Enable** the option **Enable third-party browser extensions.** Click **OK.** Go to **Tools ⊙ Internet Options**. Select the **Security** tab. Select **security zone** and adjust settings for this zone. Recommended is **Trusted Sites**

e) Click **OK**

10. ActiveX Controls

a) Go to **Tools ⊙ Internet Options ⊙ Select Security Tab ⊙ Select Internet zone**
b) Click on Custom level button
c) Set to Enable the **option Run ActiveX controls and plug-ins** and **Script ActiveX controls marked safe for scripting*** under **ActiveX controls and plug-ins**.
d) Click **OK**

11. Clear History

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

12. Configure workstation Java plug-in for ProAlarm

Note: The minimum requirement for executing Proalarm Applets on a web Browser: IE 6.0 (JRE Plugin for Internet Explorer with Java 1.5 plug-in. For Applet Runtime Settings, In the Java Control Panel, we need to set the applet runtime parameters in order to get a better performance. These Runtime settings will be used when proalarm is executed in the browser. This must be applied before starting the Browser:

a) Go to **Start Menu ⊙ Settings ⊙ Control Panel ⊙ Java Plug-in**
b) Click on the **Advanced tab**
c) Here, you will find Java Runtime parameters, in which you can assign the given value

```
-Xms400m -Xmx640m
```

CAUTION: If your workstation cannot allocate this amount of memory, IE will crash. In that case, try this: `-Xms256m -Xmx512m`

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

13. Compatibility view

Note: This step need 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.

15 PIC Bulkconfig File Description

15.1 NSP Bulkconfig File Description

The NSP subsystem `bulkconfig` file contains the overall NSP pre-installation configuration information, most importantly the hostname and SNMP configuration. During the installation process, various scripts use this file to configure NSP.

The bulkconfig file is a text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The bulkconfig file templates can be found on the NSP iso in the `/` directory. For NSP One-Box you can use the `/bulkconfig.nsp-onebox` template together with the `/bulkconfig.example.nsp-onebox` example showing an updated bulkconfig template. Do not use this reference example to configure the NSP system. For NSP Four-Box you can use the

/bulkconfig.nsp-fourbox template together with the /bulkconfig.example.nsp-fourbox example.

Note: When you install PIC, you are asked to create this bulkconfig file and update this file. **DO NOT** remove the NSP bulkconfig file from the server.

This topic provides a description of each keyword and parameter used in the bulkconfig file. It is important to read and understand the contents of this file.

bulkconfig file location and rights

File name: bulkconfig

File absolute path: /root/bulkconfig

Note: If the bulkconfig file is copied form ISO and moved to the /root , the permission will be Readonly. In this case change the rights to match the example below.

```
[root@nsponebox~]# pwd
/root
[root@nsponebox ~]# ls -l | grep bulkconfig
-rw-r--r-- 1 root root   358 Dec  4 19:20 bulkconfig
```

bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword, and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_gat
eway
ntpserver1,IP_address
ntpserver2,IP_address
timezone,time_zone
```

Refer to the following descriptions of each keyword and its associated values.

host Description

```
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_gat
eway
...
```

Example (Four-Box Configuration):

```
host,nsp-apache,10.236.2.141,NSP_APACHE,eth01,255.255.255.224,10.236.2.129
host,nsp-apache,10.236.1.141,NSP_APACHE,eth02,255.255.255.224,10.236.1.129
host,nsp-oracle,10.236.2.142,NSP_ORACLE,eth01,255.255.255.224,10.236.2.129
host,nsp-secondary,10.236.2.143,NSP_SECONDARY,eth01,255.255.255.224,10.236.2.129
host,nsp-primary,10.236.2.144,NSP_PRIMARY,eth01,255.255.255.224,10.236.2.129...
```

There is single host line for each server except for the NSP Apache.

The host keyword has the following associated values:

hostname_of_server ***function***

IP_address

A valid hostname , it should match the hostname set on server.

The IP address of the server. For blade systems, the internal IP address of the server.

interface_name

The function of the server. Use one of the following entries:

- `NSP_ONEBOX` for the NSP One-box Server
- `NSP_APACHE` for the NSP Apache Server
- `NSP_ORACLE` for the NSP Oracle Server
- `NSP_SECONDARY` for the NSP Secondary Server
- `NSP_PRIMARY` for the NSP Primary Server

network_mask

network_gateway

Name of the interface where the network settings are applied.

- Use `eth01` for a rackmount system and `eth02` for the second interface on Apache and One-box servers.
- Use `bond0.3` for the blade systems and `bond0.4` for the second interface on Apache and One-box servers.

The network mask.

The default gateway.

ntpserver Description

```
ntpserver1,IP_address
ntpserver2,IP_address
```

- `ntpserver1` is the first NTP server
- `ntpserver2` is the second NTP server

Example:

```
ntpserver1,10.236.129.11
ntpserver2,
```

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server.

timezone Description

```
timezone,time_zone
```

Example:

```
timezone,Europe/Prague
```

The timezone keyword has the following associated value:

time_zone The timezone string. For a list of available timezones that you can use, refer to the `/usr/share/zoneinfo/zone.tab` file **TZ** column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT--
#code   coordinates     TZ                      comments
AD      +4230+00131     Europe/Andorra
AE      +2518+05518     Asia/Dubai
AF      +3431+06912     Asia/Kabul
AG      +1703-06148     America/Antigua
CZ      +5005+01426     Europe/Prague
---CUT—
```

NSP One-box

`bulkconfig` Template

```
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_ga
teway
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_ga
teway ntpserver1,IP_address
ntpserver2,IP_addres
s timezone,time_zone
```

Example:

A `bulkconfig` file needs to be created for the NSP One-box:

- Server hostname: `nsp-onebox`
- Because it is a one-box server, two interfaces are needed
- Because it is a rackmount system, use `eth01` and `eth02` for these interfaces

  Note: If you are configuring C-class blades, replace `eth01` with `bond0.3` and `eth02` with `bond0.4`
  when you create this file.

- IP addresses:
  - First interface (`eth01`): `10.236.2.141`
  - Second interface (`eth02`): `10.236.1.141`
- Subnet mask: `255.255.255.254`
- Gateway addresses:
  - First interface (`eth01`): `10.236.2.129`
  - Second interface (`eth02`): `10.236.1.129`
- NTP server IP address: `10.236.129.11`
- Server timezone: `Europe/Prague`

The corresponding `bulkconfig` file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@nsp-onebox ~]# cat /root/bulkconfig
host,nsp-
onebox,10.236.2.141,NSP_ONEBOX,eth01,255.255.255.224,10.236.2.129
host,nsp-
onebox,10.236.1.142,NSP_ONEBOX,eth02,255.255.255.224,10.236.1.129
ntpserver1,10.236.129.11
ntpserver2,
timezone,Europe/Pragu
e
```

`bulkconfig` Template

```
host,hostname_apache,IP_address,function,interface_name,network_mask,network_gatew
ay
host,hostname_apache,IP_address,function,interface_name,network_mask,network_gatew
ay
host,hostname_oracle,IP_address,function,interface_name,network_mask,network_gatew
ay
host,hostname_secondary,IP_address,function,interface_name,network_mask,network_ga
teway
host,hostname_primary,IP_address,function,interface_name,network_mask,network_gate
way ntpserver1,IP_address
ntpserver2,IP_addres
s timezone,time_zone
```

Example:

A `bulkconfig` file needs to be created for the NSP cluster setup with four physical servers:

- Server hostname: `nsp-apache`
- Server hostname: `nsp-oracle`
- Server hostname: `nsp-secondary`
- Server hostname: `nsp-primary`
- Because it is a rackmount system, use `eth01` and `eth02` for interface names

  Note: If you are configuring C-class blades, replace `eth01` with `bond0.3` and `eth02` with `bond0.4`
  when you create this file.

- Apache IP addresses:
  - First interface (`eth01`): `10.236.2.141`
  - Second interface (`eth02`): `10.236.1.141`
- Oracle IP address (`eth01`): `10.236.2.142`
- Secondary IP address (`eth01`): `10.236.2.143`
- Primary IP address (`eth01`): `10.236.2.144`
- Subnet mask: `255.255.255.254`
- Gateway addresses:
  - Apache `eth01`: `10.236.2.129`
  - Apache `eth02`: `10.236.1.129`
  - Default for all other servers: `10.236.2.129`
- NTP server IP address: `10.236.129.11`
- Server timezone: `Europe/Prague`

The corresponding `bulkconfig` file you create should appear as follows:

Note: There is no new line character in the middle of host configuration, and there should not be any typos in bulkconfig file.

```
[root@nsp ~]# cat /root/bulkconfig
host,nsp-apache,10.236.2.141,NSP_APACHE,eth01,255.255.255.224,10.236.2.129
host,nsp-apache,10.236.1.141,NSP_APACHE,eth02,255.255.255.224,10.236.1.129
host,nsp-oracle,10.236.2.142,NSP_ORACLE,eth01,255.255.255.224,10.236.2.129
host,nsp-
secondary,10.236.2.143,NSP_SECONDARY,eth01,255.255.255.224,10.236.2.129
host,nsp-primary,10.236.2.144,NSP_PRIMARY,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
ntpserver2
,
```

```
ntpserver3
,
timezone,Europe/Prague
```

15.2 IXP Bulkconfig File Description

The IXP subsystem `bulkconfig` file contains the overall IXP pre-installation configuration information. During the installation process, various scripts use this file to configure IXP.

The bulkconfig file is a case sensitive text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The IXP bulkconfig file template is located on the IXP iso on the `/upgrade/IXP_bulkconfig_template` path.

The file is unique for the IXP subsystem and is present on each server in this subsystem.

Note: When you install PIC, you are asked to create this `bulkconfig` file and update this file. **DO NOT** remove the IXP `bulkconfig` file from the server.

The IXP subsystem `bulkconfig` file is used during these processes:

- Manufacturing installation
- Customer network integration
- Change IP
- Disaster recovery procedure
- RSP install/upgrade procedure

This topic provides a description of each keyword and parameter used in the `bulkconfig` file. It is important to read and understand the contents of this file.

`bulkconfig` file location and rights

File name: bulkconfig

File absolute path: `/root/bulkconfig`

Note: If the bulkconfig file is copied form ISO and moved to the /root , the permission will be Readonly. In this case change the rights to match the example below.

```
[root@ixp1981-1a ~]# pwd
/root
```

```
[root@ixp1981-1a ~]# ls -l | grep bulkconfig
-rw-r--r-- 1 root root   358 Dec  4 19:20 bulkconfig
```

`bulkconfig` file: template

The `bulkconfig` file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword, and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_1st_server,IP_address,function,interface_name,network_mask,networ
k_gateway
```

```
host,hostname_of_2nd_server,IP_address,function,interface_name,network_mask,networ
k_gateway
host,hostname_of_nth_server,IP_address,function,interface_name,network_mask,networ
k_gateway ntpserver1,IP_address
ntpserver2,IP_addres
s
ntpserver3,IP_addres
s ntppeerA,
ntppeerB,
nspprimary,IP_address_of_primary_weblogic_or_onebox_ns
p nspsecondary,IP_address_of_secondary_weblogic
nsporacle,IP_address_of_oracle_server
timezone,time_zone
```

Refer to the following descriptions of each keyword and its associated values.

host Description

```
host,hostname_of_1st_server,IP_address,function,interface_name,network_mask,networ
k_gateway
host,hostname_of_2nd_server,IP_address,function,interface_name,network_mask,networ
k_gateway
host,hostname_of_nth_server,IP_address,function,interface_name,network_mask,networ
k_gateway
...
```

Example (installation):

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

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

Example (disaster recovery of `ixp1981-1b` server):

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

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

The host keyword has the following associated values:

hostname_of_nth_server	The server hostname in the standard IXP format: ixp*NNNN-MA* where: • *N* is numeric 0-9 • *M* is numeric 1-9 • *A* is alphabetical a-z **Note:** This bulkconfig is either used for the Report Server installation. All Report Servers must be installed with 1a designation
IP_address	The IP address of the server. For blade systems, the internal IP address of the server
function	The function of the server. Use one of the following entries for installation: • IXP-XDR for the xDR Storage Server and

	Primary Report Server • IXP-PDU for the PDU Storage Server • IXP-BASE for the IXP Base Server, Cluster Report Server and PPS server • IXP-ES for the Export Server Function for the disaster recovery procedure for the particular server is different. Use one of the following entries for disaster recovery: • DR-XDR for the xDR Storage Server • DR-PDU for the PDU Storage Server • DR-BASE for the IXP Base Server • DR-ES for the Export Server
interface_name	Name of the interface where the network settings are applied. • eth01 for the rackmount systems • bond0.3 for the blade systems
network_mask	The network mask
network_gateway	The default gateway

.

ntpserver Description

```
ntpserver1,IP_address
ntpserver2,IP_address
ntpserver3,IP_address
ntppeerA,
ntppeerB,
```

- `ntpserver1` is the first NTP server
- `ntpserver2` is the second NTP server
- `ntpserver3` is the third NTP server
- `ntppeerA` not applicable; leave empty
- `ntppeerB` not applicable; leave empty

Example:

```
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
```

The ntpserver keyword has the following associated value:

IP_address	The IP address of the NTP server.

NSP Description

```
nspprimary,IP_address_of_primary_weblogic_or_onebox_nsp
nspsecondary,IP_address_of_secondary_weblogic
nsporacle,IP_address_of_oracle_server
```

- `nspprimary` is the NSP Primary WebLogic server or the One-box NSP server
- `nspsecondary` is the NSP Secondary WebLogic server
- `nsporacle` is the NSP Oracle server

Example (for a One-box NSP):

```
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
```

The NSP keyword has the following associated values:

IP_address_of_primary_weblogic_or_onebox_nsp	The IP address of the NSP server: • One-box: IP address of the One-box NSP server • Four-box: IP address of the NSP Primary WebLogic server
IP_address_of_secondary_weblogic	The IP address of the NSP server: • One-box: not applicable; leave empty • Four-box: IP address of the NSP Secondary WebLogic server

IP_address_of_oracle_server :

:

The IP address of the NSP Oracle server

- One-box: not applicable; leave empty
- Four-box: IP address of the NSP Oracle server

timezone Description

```
timezone,time_zone
```

Example:

```
timezone,Europe/Prague
```

The timezone keyword has the following associated value:

time_zone

The timezone string. For a list of available timezones that you can use, refer to the `/usr/share/zoneinfo/zone.tab` file **TZ** column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT--
#code   coordinates     TZ                    comments
AD      +4230+00131     Europe/Andorra


AE      +2518+05518     Asia/Dubai
AF      +3431+06912     Asia/Kabul
AG      +1703-06148     America/Antigua
CZ      +5005+01426     Europe/Prague
---CUT—
```

`bulkconfig` file: installation example

A `bulkconfig` file needs to be created for the following IXP subsystem:

- Subsystem hostname: `ixp1981`
- 1a server is the xDR Storage Server with the IP address: `10.236.2.141`
- 1b server is the Base Server with the IP address: `10.236.2.142`
- 1c server is the PDU Storage Server with the IP address: `10.236.2.143`
- Network interface: `eth01`
- Network mask: `255.255.255.254`
- Default gateway: `10.236.2.129`
- NTP server IP address: `10.236.129.11`
- NSP One-box IP address: `10.10.10.10`
- Server timezone: `Europe/Prague`

The corresponding `bulkconfig` file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@ixp1981-1a ~]# cat /root/bulkconfig
host,ixp1981-1a,10.236.2.141,IXP-XDR,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,IXP-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-PDU,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
timezone,Europe/Prague
```

Automated records in `/etc/bulkconfig` file

During the automated integration of IXP subsystem with EFS server(s) the following line is added to the `/etc/bulkconfig` file (one per integrated EFS server):

```
efs,hostname_of_EFS,IP_address_of_EFS
```

where

- *hostname_of_EFS* is the hostname of EFS that local DataFeeds hosts uses as an export target
- *IP_address_of_EFS* is the IP address of such

EFS Example:

```
efs,ixp7777-1e,10.236.0.33
```

15.3 EFS Bulkconfig File Description

The standalone Export File Server (EFS) `bulkconfig` file contains the overall EFS pre-installation configuration information. During the installation process, various scripts use this file to configure the EFS server.

The bulkconfig file is a case sensitive text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The EFS bulkconfig file template is located on the EFS iso on the `/upgrade/EFS_bulkconfig_template` path.

For the EFS server, you must create a new and unique `bulkconfig` file. Do **not** reuse the `bulkconfig` file that was created for the servers in the IXP subsystem.

Note: When you install PIC, you are asked to create this `bulkconfig` file and update this file. **DO NOT** remove the EFS `bulkconfig` file from the server.

The EFS `bulkconfig` file is used during these processes:

- EFS Manufacturing installation
- Customer network integration
- Change IP

This topic provides a description of each keyword and parameter used in the `bulkconfig` file. It is important to read and understand the contents of this file.

`bulkconfig` file location and rights

File name: bulkconfig

File absolute path: /root/bulkconfig

Note: If the bulkconfig file is copied form ISO and moved to the /root , the permission will be Readonly. In this case change the rights to match the example below.

```
[root@ixp1981-1a ~]# pwd
/root
[root@ixp1981-1a ~]# ls -l | grep bulkconfig
-rw-r--r-- 1 root root   358 Dec  4 19:20 bulkconfig
```

`bulkconfig` file: template

The `bulkconfig` file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword, and then contains various values for

this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_efs_server,IP_address,function,interface_name,network_mask,network
_gateway
ntpserver1,IP_address
ntpserver2,IP_address
ntpserver3,IP_address
ntppeerA,
ntppeerB,


nspprimary,IP_address_of_primary_weblogic_or_onebox_nsp
nspsecondary,IP_address_of_secondary_weblogic
nsporacle,IP_address_of_oracle_server
timezone,time_zone
```

Refer to the following descriptions of each keyword and its associated values.

host Description

```
host,hostname_of_efs_server,IP_address,function,interface_name,network_mask,network
_gateway
...
```

Example (installation):

```
host,ixp1981-1a,10.236.2.141,EFS,eth01,255.255.255.224,10.236.2.129
```

Example (disaster recovery):

```
host,ixp1981-1a,10.236.2.141,DR-EFS,eth01,255.255.255.224,10.236.2.129
```

The host keyword has the following associated values:

hostname_of_efs_server	The server hostname in the standard IXP format: ixp*NNNN-MA* where: • *N* is numeric 0-9 • *M* is numeric 1-9 • *A* is alphabetical a-z **Note:** This bulkconfig is either used for the Report Server installation. All Report Servers must be installed with 1a designation.
IP_address	The IP address of the server.
function	The function of the server. Use `EFS`.
interface_name	Name of the interface where the network settings are applied. Use `eth01` for the rackmount system.
network_mask	The network mask.
network_gateway	The default gateway.

ntpserver Description

```
ntpserver1,IP_addres
s
ntpserver2,IP_addres
s
ntpserver3,IP_addres
s ntppeerA,
ntppeerB,
```

- `ntpserver1` is the first NTP server
- `ntpserver2` is the second NTP server
- `ntpserver3` is the third NTP server
- `ntppeerA` not applicable; leave empty
- `ntppeerB` not applicable; leave empty

Example:

```
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
```

The ntpserver keyword has the following associated value:

IP_address	The IP address of the NTP server.

NSP Description

```
nspprimary,IP_address_of_primary_weblogic_or_onebox_nsp
nspsecondary,IP_address_of_secondary_weblogic
nsporacle,IP_address_of_oracle_server
```

- `nspprimary` is the NSP Primary WebLogic server or the One-box NSP server
- `nspsecondary` is the NSP Secondary WebLogic server
- `nsporacle` is the NSP Oracle server

Example (for a One-box NSP):

```
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
```

The NSP keyword has the following associated values:

IP_address_of_primary_weblogic_or_onebox_nsp	The IP address of the NSP server: • One-box: IP address of the One-box NSP server • Four-box: IP address of the NSP Primary WebLogic server
IP_address_of_secondary_weblogic	The IP address of the NSP server: • One-box: not applicable; leave empty • Four-box: IP address of the NSP Secondary WebLogic server

IP_address_of_oracle_server The IP address of the NSP Oracle server:

- One-box: not applicable; leave empty
- Four-box: IP address of the NSP Oracle server

timezone Description

```
timezone,time_zone
```

Example:

```
timezone,Europe/Prague
```

The timezone keyword has the following associated value:

time_zone

The timezone string. For a list of available timezones that you can use, refer to the `/usr/share/zoneinfo/zone.tab` file **TZ** column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT--
#code   coordinates     TZ                    comments
AD      +4230+00131     Europe/Andorra
AE      +2518+05518     Asia/Dubai
AF      +3431+06912     Asia/Kabul
AG      +1703-06148     America/Antigua
CZ      +5005+01426     Europe/Prague
---CUT—
```

`bulkconfig` file: example

A `bulkconfig` file needs to be created for the following EFS:

- EFS server hostname: `ixp1981-1a`
- EFS server IP address: `10.236.2.141`
- Network interface: `eth01`
- Network mask: `255.255.255.254`
- Default gateway: `10.236.2.129`
- NTP server IP address: `10.236.129.11`
- NSP One-box IP address: `10.10.10.10`
- Server timezone: `Europe/Prague`

The corresponding `bulkconfig` file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@ixp1981-1a ~]# cat /root/bulkconfig
host,ixp1981-1a,10.236.2.141,EFS,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
nspprimary,10.10.10.10
nspsecondary,


nsporacle,
timezone,Europe/Pragu
```

e

Automated records in /etc/bulkconfig file

During the automated integration of EFS server with IXP subsystem the following line is added to the /etc/bulkconfig file (one per IXP DataFeed hosts server):

```
ixp,hostname_of_IXP,IP_address_of_IXP
```

where

- *hostname_of_IXP* is the hostname of IXP server that hosts DataFeed application.
- *IP_address_of_IXP* is the IP address of such IXP server

Example:

```
ixp,ixp7777-1a,10.236.0.33
```

15.4 xMF Bulkconfig *File Description*

This topic describes the syntax and use of the xMF bulkconfig file.
The xMF subsystem bulk configuration file contains the overall xMF subsystem configuration information. The bulkConf.pl script uses this single file to configure the xMF subsystem accordingly. The bulkconfig file is a text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The xMF bulkconfig file template is located on the XMF server on the /usr/TKLC/plat/etc/platform.csv path. Example of bulkconfig file is locate on the /usr/TKLC/plat/etc/platform.example.csv path. Do not use this reference example to configure the xMF server!

The file is unique per subsystem and is present on each server in the subsystem.

DO NOT remove the xMF bulkconfig file from the server or subsystem.

This topic provides a description of each keyword and parameter used in the bulkconfig file (platform.csv). It is important to read and understand the contents of this file.

Bulkconfig file location and rights

File name: platform.csv

File path:/var/TKLC/upgrade/platform.csv

Bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_1st_server,function,designation,interface_name,IP_address,network_mask,network_gateway
host,hostname_of_2nd_server,function,designation,interface_name,IP_address,network_mask,network_gateway
host,hostname_of_nth_server,function,designation,interface_name,IP_address,network_mask,network_gateway
```

```
ntp,ntpserver1,IP_address
ntp,ntpserver2,IP_address
ntp,ntpserver3,IP_address
ntp,ntppeerA,IP_address
ntp,ntppeerB,IP_address
app,appserver,IP_address_of_primary_nsp
app,appserver2,IP_address_of_secondary_ns
p tz,time_zone
```

Refer to the following descriptions of each keyword and its associated values.

host Description

```
host,hostname_of_1st_server,function,designation,interface_name,IP_address,network
_mask,network_gateway
host,hostname_of_2nd_server,function,designation,interface_name,IP_address,network
_mask,network_gateway
host,hostname_of_nth_server,function,designation,interface_name,IP_address,network
_mask,network_gateway
...
```

Example for IMF setup:

```
host,imf-
1a,IMF,1A,bond0.200,192.168.253.5,255.255.255.224,192.168.253.1
host,imf-
1b,IMF,1B,bond0.200,192.168.253.6,255.255.255.224,192.168.253.1
host,imf-
1c,IMF,1C,bond0.200,192.168.253.7,255.255.255.224,192.168.253.1
```

Example for PMF standalone:

```
host,pmf-0a,PMF,0A,eth01,192.168.2.106,255.255.255.0,192.168.2.1
```

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

The host keyword has the following associated values:

hostname_of_nth_server	The server hostname. **Note:** It is recommended that the hostname ends with the designation of the server (for example, malibu-1a).
function	The function of the server. Use one of the following entries: • IMF • PMF
designation	The designation of the server is a combination of frame number and position of the server in the frame. Use the following rule: • xMF subsystem: 1A for the first server, 1B for the second server, etc. • PMF standalone: 0A
interface name	The name of customer network interface (typically: bond0.200 for IMF and eth01 for PMF)
IP_address	The IP address of the server. For blade systems, the internal IP address of the server
network_mask	The network mask
network_gateway	The default gateway

ntpserver Description

```
ntp,ntpserver1,IP_address
ntp,ntpserver2,IP_address
ntp,ntpserver3,IP_address
ntp,ntppeerA,IP_address
ntp,ntppeerB,IP_address
```

- `ntpserver1` is the first NTP server
- `ntpserver2` is the second NTP server
- `ntpserver3` is the third NTP server
- `ntppeerA` not applicable; leave empty
- `ntppeerB` not applicable; leave empty

Example:

```
ntp,ntpserver1,10.236.129.11
```

The ntpserver keyword has the following associated value:

IP_address	The IP address of the NTP server.

nsp Description

```
app,appserver,IP_address_of_primary_nsp
app,appserver2,IP_address_of_secondary_nsp_appserver
```

- `appserver` is the NSP Primary server
- `appserver2` is the NSP Secondary WebLogic server

Example (for a One-box NSP):

```
app,appserver,10.10.10.10
```

The nsp keyword has the following associated values:

IP_address_of_primary_nsp	The IP address of the NSP Primary server: • One-box: IP address of the One-box NSP server • Four-box: IP address of the NSP Primary server
IP_address_of_secondary_nsp	The IP address of the NSP Secondary server: • One-box: not applicable; leave empty • Four-box: IP address of the NSP Secondary server

timezone Description

```
timezone,time_zone
```

Example

```
timezone,Europe/Prague
```

The timezone keyword has the following associated value:

Time_zone *The* timezone string. For a list of available timezones that you can use, refer to the/usr/share/zoneinfo/zone.tab file **TZ** column. For example

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT--
#code   coordinates     TZ                    comments
AD      +4230+00131     Europe/Andorra
AE      +2518+05518     Asia/Dubai
AF      +3431+06912     Asia/Kabul
AG      +1703-06148     America/Antigua
CZ      +5005+01426     Europe/Prague
---CUT—
```

Bulkconfig file: example

A bulkconfig file needs to be created for the following xMF subsystem:

- Subsystem hostname: `imf-1a`
- 1a server with the IP address: `192.168.253.5`
- 1b server with the IP address: `192.168.253.6`
- 1c server with the IP address: `191.168.253.7`
- IMF subsystem, interface: `bond0.200`
- Network mask: `255.255.255.224`
- Default gateway: `192.168.253.1`
- NTP server IP address: `10.250.32.10`
- Subsystem is added to the appserver with IP address: `10.10.10.10`
- Subsystem timezone: `Europe/Prague`

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@T3-1A upgrade]# cat platform.csv
host,imf-1a,IMF,1A,bond0.200,192.168.253.5,255.255.255.224,192.168.253.1
host,imf-1b,IMF,1B,bond0.200,192.168.253.6,255.255.255.224,192.168.253.1
host,imf-1c,IMF,1C,bond0.200,192.168.253.7,255.255.255.224,192.168.253.1
ntp,ntpserver1,10.250.32.10
ntp,ntpserver2,10.250.32.11
ntp,ntpserver3,10.250.32.12
ntp,ntppeerA,10.250.32.13
ntp,ntppeerB,10.250.32.14
app,appserver,10.10.10.10
app,appserver2,10.10.10.11
tz,Europe/Prague
```

16 Knowledge Base Procedures

16.1 How to connect to the console via the MRV

1. **Telnet to the console via the MRV**

   a) Connect using ssh where <port> comes from the list below below and <mrv_address> is the IP address of the MRV.

   ```
   # ssh tklc@<mrv_address> -p <port>
   ```

Table 2: DCL Table 1

Target Designation	MRV port
xA (server1)	2122
xB (server2)	2222
xC (server3)	2322
xD (server4)	2422
xE (server5)	2522
Yellow switch	2722
Blue switch	2822

2. Connect to the console via the MRV

a) Connect using ssh where <port> comes from the list below and <mrv_address> is the IP address of the MRV.

```
# ssh tklc@<mrv_address> -p <port>
```

b) If this is the first time connecting to the server, answer `yes` to exchange secure keys.

```
The authenticity of host 'earthoobm1a (192.168.62.200)' can't be
established. RSA key fingerprint is
38:9f:5c:31:6c:e6:7a:a9:43:9f:a7:0a:77:7d:42:da.
Are you sure you want to continue connecting (yes/no)?
yes
```

c) At the password prompt type the tklc user's password and press `<enter>`

d) Press `<enter>` to get a login prompt.

e) Verify the Login prompt displays the desired hostname

3. When finished use the following key sequence to exit the oobm.

(Enter followed by Tilde).

a) Type

```
exit
```

b) Press `<enter>` and `<shift>+<~>+<.>`

16.2 How to connect to RMM

This procedure describes the steps to verify connectivity to the RMM on the Tek 3 server.

Connect to RMM

a) Open internet explorer and navigate to the IP address of the RMM

b) Log into the RMM. The default username is admin and the default password is password. c) Open Remote Console by click on Remote Console > KVM Console

t**Note:** You might need to accept and java message on your 1st time connecting.

16.3 How to connect to the console via OOBM

If you are unable to connect to OOBM w/ IP run the following steps:

Connect to OOBM

a) Check if the OOBM has console set for remote or local. At the Choice prompt, type **1** and press `<enter>`

```
-----------------
Command Interface
-----------------
Please enter your choice:
1. Run Localcuri
2. Start Serial Port Redirection
Choice (1 or 2)? 1
```

Output:

```
CURI Client - command line utility Version 1.16.0
Copyright (c) 2003-2004 American Megatrends Inc., Norcross GA.

Type 'exit'/'quit' to exit the CURI prompt

Enter CURI command (Logged in as root, Administrator) :
```

b) At the prompt, type the command to get the status of the console

```
GetSerialAccessCfg
```

Output:

```
   Serial Port Access is currently set to Local.
```

c) If serial port access is set to Local, change to remote, otherwise skip to the next step.

```
GetSerialAccessCfg  SetSerialAccessCfg Remote
```

Output:

```
   Serial Port Access configuration has been changed successfully.
```

Return to previous step to verify change.

d) Press **<enter>** to get back to Command Interface menu again.

Output:

```
----------------
- Command
Interface
-----------------
Please enter your choice:
1. Run Localcuri
2. Start Serial Port Redirection
Choice (1 or 2)?
```

e) Type **2** and press **<enter>** to connect to serial console.

16.4 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.

16.5 Configure and Verify iLO Connection

This procedure is applicable to HP DL360, ML350, DL380 G4 and G5 servers (IXP, NSP and Standalone PMF)

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 create 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.

Open Internet Explorer

a) Open Internet Explorer on a workstation and enter in the iLo IP address.

http://192.168.120.12

Where 192.168.120.12 is the IP address of the

iLo. b) You will get a SSL security warning

c) Accept the warning.

d) Fill in **Login name** and **Password** and enter the iLO.

e) Once you are logged in click on Launch to start Integrated Remote Console. f) If you will receive another certificate warning click on **Yes** to continue

g) If you get **The application's digital signature can not be verified** click **Always trust content from this publisher** then click **Run**.

h) A remote console window will now appear to allow you to access the HP server.

16.6 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.

   Alternatively:

   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:

   a) cd into the directory where your ISO image is located (not on the PM&C server)

   b) Using sftp, connect to the PM&C management server

      > **sftp pmacftpusr@<PM&C_management_network_IP>**

      > **put <image>.iso**

   c) After the image transfer is 100% complete, close the connection

      > **quit**

   Refer to the documentation provided by application for pmacftpusr password.

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

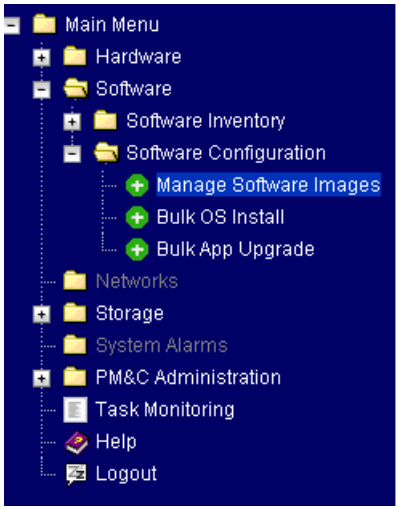
   Open web browser and enter:

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

   Login as pmacadmin user.

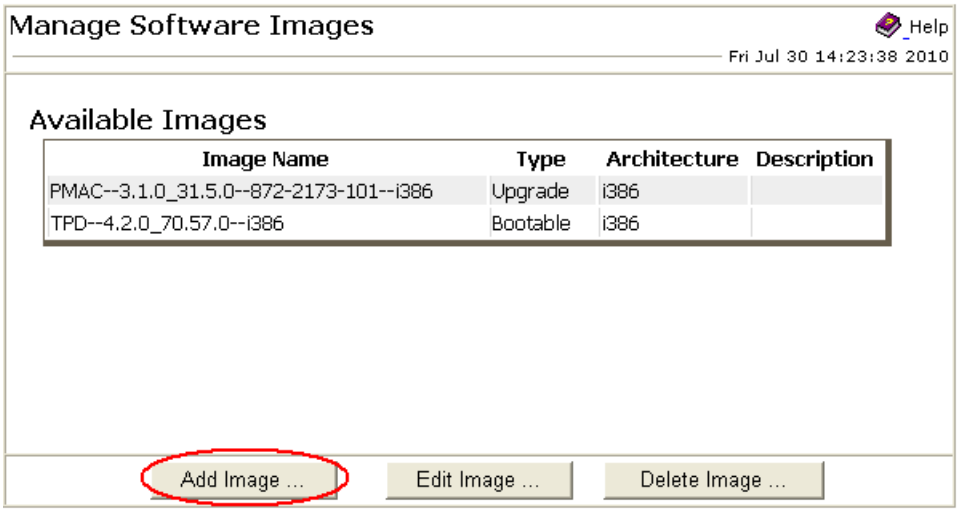
3. **PM&C GUI: Navigate to Manage Software Images**

   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.

16.7 Reconfigure System Disk Array on HP Rackmount G5 Servers

This procedure describes how to configure system disks before the operating system is reinstalled. This procedure is applicable to rackmount HP G5 servers. Use this procedure only if automated configuration that is part of IPM on G5 servers failed.

1. **Power on the server**

   a) Power on the server and wait for the following message :

```
Slot 0 HP Smart Array p400i Controller (256MB, v4.12 Logical Drive
Press  <F8>
to run the  option ROM
 Configuration for Arrays
Utility
Press  <Esc>
 to skip configuration and continue
```

Note: Slot 0 have to be present on this screen. It indicates internal

controller. b) Press the <F8> key.

Note: without an operator action in a few seconds, the system continues automatically with the default choice, which corresponds to <Esc> which means skip. If this happens, you must power off and restart this step.

2. Cleanup existing drives

a) Navigate to **View Logical Drive**.

b) Execute on of the following choises:

- If a previous configuration exists and if it's not a RAID1 navigate to **Delete Logical Drive and** delete the existing configuration.
- If the server has already a RAID1 configuration press [Esc]

3. Create system logical drive

Note: This step is applicable only if you have deleted the existing drives in the previous step.

a) Navigate to **Create Logical Drive**.

b) The screen displays a list of available physical drives and the valid RAID options for the system. c) Use the <Arrow> keys, <Spacebar>, and <Tab> keys to navigate around this screen and set
up the logical drive RAID 1+0.

d) Uncheck **Spare** selection.

e) Maximum boot partition set to **Disabled (4GB)**

f) Move to the settings that allows either 4 GB or 8 GB as the maximum boot drive size, select **4 GB**.

g) Press the <ENTER> key to accept the settings.

h) Press the <F8> key to confirm the settings and save the new configuration. i) After several seconds, the Configuration Saved screen comes up again.

j) Press the <ENTER> key to continue.

k) Press the <ESC> key to quit and continue boot.

4. Correct boot controller order

Note: This step is applicable only if the external disk storage is attached to the

server. a) Wait for the following message:

```
Slot 2 HP Smart Array 6400 Controller (192MB, v2.44)  0
Logical Drive
Press  <F8>
to run the  option ROM
 Configuration for Arrays
Utility
Press  <Esc>
```

```
to skip configuration and continue
```

b) Hit <Esc> to continue

c) Wait until the server will boot to the following message:

```
Press "F9" key for ROM-based Setup Utility
Press "F10" key for System Maintenance
Menu Press "F12" key for PXE boot
```

d) Press <F9> to enter **ROM-Based Setup Utility**

e) Select **Boot Controller Order** option and press <ENTER>.

f) Make sure that on the first line is **Embedded HP Smart Array** controller. g) Press <ESC> to return to the main menu.

Leave the menu.

16.8 How to remove IP Address and Route

This procedure describes how to remove the IP address and Route in case of both Rackmount and Blade Servers.

1. **Follow the Steps below for Rackmount Servers only**

Note: Remove any physical cabling for the IP interface to be removed before running steps below. a) Open a terminal window and log in as root user .

b) Execute the command given below

```
# platcfgadm --show NCRoutes NCInterfaces
```

```
# ifconfig interface_name down
```

where *interface_name* will be the interface needs to be removed e.g eth02

c) Enter the **platcfg** menu. As root, run:

```
# su – platcfg
```

d) From main **platcfg** menu, select **Network Configuration ⊙ Routing ⊙ IPv4 ⊙ Static Routes ⊙ Display Table ⊙ main ⊙ Edit ⊙ Delete Route**. e) Select Route to be deleted and Press [Enter] .

Note: If there is only single (default) route available. Do not delete that route.

f) From main **platcfg** menu, Select **Network Configuration ⊙ Network Interfaces ⊙ IPv4 ⊙** Edit an Interface .

g) Select the *interface_name* needs to removed . For e.g eth02

h) Select **OK** and press **ENTER**.

i) Select Boot Protcol as **none** and press **ENTER**

j) Choose Address Action as **Delete** and press **ENTER**

k) Select IPv4 Address to delete and select "OK" then press **ENTER** l) Select "Exit" and press **ENTER** repetitively to exit Platcfg Menu . m) Run following command

```
# platcfgadm --hide NCRoutes NCInterfaces
```

n) Use *ifconfig* command to verify IP address removed is no longer visible.

2. **Follow the steps below for Blade Servers only.**

a) Open a terminal window and log in as root user .

b) Execute the command given below

```
# platcfgadm --show NCRoutes NCInterfaces
```

```
# ifconfig interface_name down
```

where *interface_name* will be the interface needs to be removed e.g bond0.4

c) Enter the **platcfg** menu. As `root`, run:

```
# su – platcfg
```

d) From main **platcfg** menu, select **Network Configuration ⊙ Routing ⊙ IPv4 ⊙ Static Routes ⊙ Display Table ⊙ main ⊙ Edit ⊙ Delete Route**. e) Select Route to be deleted and Press [Enter]

Note: If there is only single (default) route available. Do not delete that route

f) From main **platcfg** menu, Select **Network Configuration ⊙ Network Interfaces ⊙ IPv4 ⊙ Delete an Interface .**

g) Select the *interface_name* needs to removed . For e.g bond0.4

h) Select **Yes** and press **ENTER**.

i) Select "Exit" and press **ENTER** repetitively to exit Platcfg Menu .

j) Run following command

```
# platcfgadm --hide NCRoutes NCInterfaces
```

k) Use *ifconfig* command to verify IP address removed is no longer visible.

16.9 How to recover a CISCO 4948 switch from the rommon prompt

In case the switch configuration failed and the switch would be in rommon follow this procedure to boot the switch

```
rommon 6 >dir bootflash:
   File size                  Checksum      File name
   ----------------------------------------------------
  12632100 bytes (0xc0c024)   0x8136853a    cat4500-ipbasek9-mz.122-31.SGA8.bin
    456060 bytes (0x6f57c)    0x66d8b2a7    cat4500-ios-promupgrade-122_31r_SGA1
   Total space = 60817408 bytes, Available = 47728992 bytes

rommon 8 >confreg
 Configuration Summary :
 => console baud: 9600
 => autoboot from: commands specified in 'BOOT' environment variable
 do you wish to change the configuration? y/n  [n]:  y
 enable  "diagnostic mode"? y/n  [n]:  n
 enable  "use net in IP bcast address"? y/n  [n]:
 enable  "load rom after netboot fails"? y/n  [n]:
 enable  "use all zero broadcast"? y/n  [n]:
 enable  "break/abort has effect"? y/n  [n]:  y
 enable  "ignore system config info"? y/n  [n]:
 change console baud rate? y/n  [n]:
 change the boot characteristics? y/n  [n]:  y
 enter to boot:
 0 = disable autoboot
 1 = the first file from internal flash device
 2 = commands specified in 'BOOT' environment variable
 [2]:
 Configuration Summary :
 => break/abort has effect
 => console baud: 9600
 => autoboot from: commands specified in 'BOOT' environment variable
```

```
 do you wish to save this configuration? y/n  [n]:  y
 You must reset or power cycle for new configuration to take effect
rommon 10 >boot bootflash:cat4500-ipbasek9-mz.122-31.SGA8.bin
Rommon reg: 0xE2004180
############
k2diags version 5.2_c
Switch> enable
Switch# config t
Switch(config)# config-reg 0x2102
Switch(config)# boot system flash bootflash:cat4500-ipbasek9-mz.122-31.SGA8.bin
Switch(config)# end
Switch# copy running-config startup-config
Switch# reload
Configuration has been modified, save?  No
<reboots>
```

The following links provide additional info if needed.
http://www.cisco.com/en/US/products/hw/switches/ps663/products_configuration_example09186a0080094ecf.shtml