DIH 1.X

DIH Installation/Upgrade Procedure

909-2232-002 Revision 1.23

April 2013

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

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*.)

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)
  - **Brazil**

    Phone:

    0-800-891-4341 (toll-free)

    TAC Regional Support Office Hours:

    8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays
  - **Chile**

    Phone:

    1230-020-555-5468
  - **Colombia**

    Phone:

    01-800-912-0537
  - **Dominican Republic**

    Phone:

    1-888-367-8552
  - **Mexico**

    Phone:

    001-888-367-8552
  - **Peru**

    Phone:

    0800-53-087
  - **Puerto Rico**

    Phone:

    1-888-367-8552 (1-888-FOR-TKLC)
  - **Venezuela**

    Phone:

0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)
  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**
  - **India**

    Phone:

    +91-124-465-5098 or +1-919-460-2150

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays
  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions

- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with the Tekelec Customer Care Center.

Related Publications

For information about additional publications that are related to this document, refer to the *Release Notice* document. The *Release Notice* document is published as a part of the *Release Documentation* and is also published as a separate document on the Tekelec Customer Support Site.

Documentation Availability, Packaging, and Updates

Tekelec provides documentation with each system and in accordance with contractual agreements. For General Availability (GA) releases, Tekelec publishes a DIH 1.x documentation set. For Limited Availability (LA) releases, Tekelec may publish a documentation subset tailored to specific feature content or hardware requirements. Documentation Bulletins announce a new or updated release.

The Tekelec DIH 1.x documentation set is released on an optical disc. This format allows for easy searches through all parts of the documentation set.

The electronic file of each manual is also available from the *Tekelec Customer Support* site. This site allows for 24-hour access to the most up-to-date documentation, including the latest versions of Feature Notices.

Printed documentation is available for GA releases on request only and with a lead time of six weeks. The printed documentation set includes pocket guides for commands and alarms. Pocket guides may also be ordered separately. Exceptions to printed documentation are:

- Hardware or Installation manuals are printed without the linked attachments found in the electronic version of the manuals.
- The Release Notice is available only on the Customer Support site.

Note: Customers may print a reasonable number of each manual for their own use.

Documentation is updated when significant changes are made that affect system operation. Updates resulting from Severity 1 and 2 Problem Reports (PRs) are made to existing manuals. Other changes are included in the documentation for the next scheduled release. Updates are made by re-issuing an electronic file to the customer support site. Customers with printed documentation should contact their Sales Representative for an addendum. Occasionally, changes are communicated first with a Documentation Bulletin to provide customers with an advanced notice of the issue until officially released in the documentation. Documentation Bulletins are posted on the Customer Support site and can be viewed per product and release.

Locate Product Documentation on the Customer Support Site

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 document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the *Tekelec Customer Support* site.

   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 **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Scope and Audience

This document describes the procedures to install the operating system and applications software on a DIH system at Release 1.x (DIH).

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

It is strongly recommended that prior to performing an installation of the operating system and applications software, 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 in the Incremental Upgrade Overview chapter that provide the sequence of the procedures for each component of this DIH system. Each procedure describes a discrete action. It is expected that the individuals responsible for upgrading the DIH system should reference these flow diagrams during this upgrade process.

Requirements and Prerequisites

Hardware Requirements

DIH release 1.x supports the following hardware for the installation: HP BL460 G6, HP BL460 Gen8*, HP DL380 Gen8*

Note: *Gen8 is supported by DIH 1.2 or later.

Software Requirements

The following software are required for the DIH 1.x installation.

Note: For specific versions and part numbers, see the DIH 1.x Release Notice.

- Tekelec Platform Distribution (TPD) (DVD or ISO file)
- Tekelec Platform Distribution (TPD) (DVD or ISO file) for TVOE host and guests
- Network Software Platform (NSP) (DVD or ISO file)
    - WebLogic (DVD or ISO file)
- Integrated xDR Platform (IXP) (CD or ISO file)
- Oracle (DVD or ISO file)
- - NGP packages for NGP software HP G6 installation
- PMF (CD or ISO file)
- xDR Builder (CD or ISO file)
- Platform Management and Configuration (PM&C) (DVD or ISO)
- Firmware update - from the Firmware management site on Sharepoint

Licenses Requirements

Licenses required for software installation of DIH 1.x are embedded licenses and do not require an explicit license key be applied. The exception to this is xDR builder license:

The following license is required for this installation:

- xDR Builder license

Chapter 2

Installation Overview

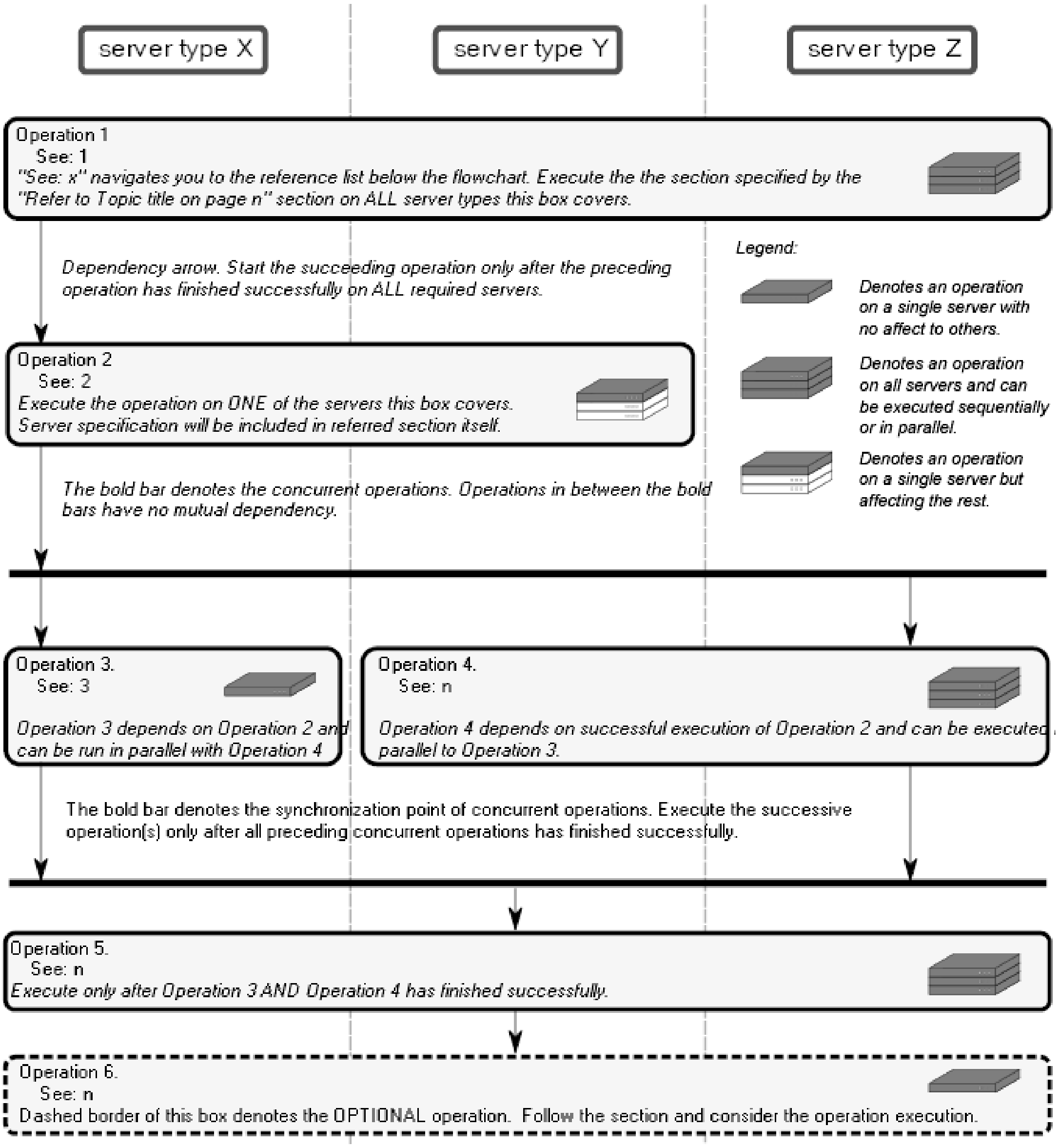
Topics:

This section provides installation overview information for the DIH system by using flowchart that depict the sequence of procedures for TVOE host and associated application guests.

Flowchart Description

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

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


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

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

DIH Installation Overview

This section provides installation overview information for the DIH system by using flowchart that depict the sequence of procedures for TVOE host and associated NSP guests.

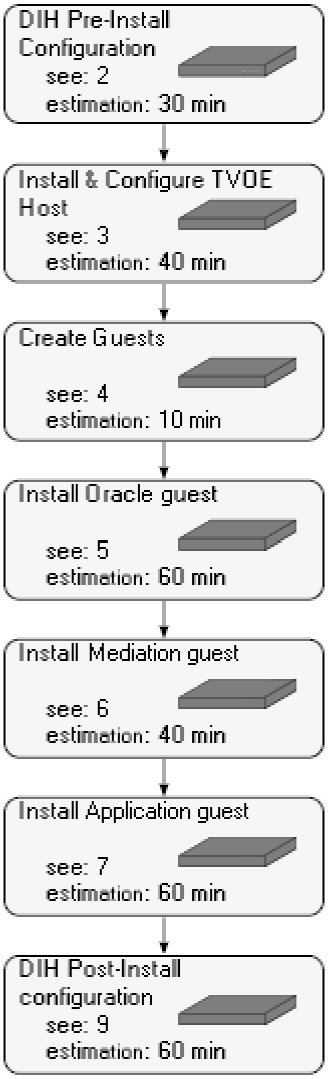
Prerequisite: PM&C and c-class blade cabinet must be already installed and configured before performing DIH installation.

The DIH system consists of the following NSP parts:

- TVOE host server
- NSP guest
- IXP guest
- PMF guest
- Oracle guest

Note: For details on the associated equipment, refer to *#unique_16*

Note: Fresh install procedure expects clean sidecar. Thus logical partitions on the external sidecar must not be created before.



1. Refer to *DIH Pre-Install Configuration*
2. Refer to *Install and Configure TVOE Host*
3. Refer to *Create and Install Operating System on guest*
4. Refer to *Install Oracle Guest*
5. Refer to *Install IXP Guest*
6. Refer to *Install NSP Guest*
7. Refer to *Install PMF guest*
8. Refer to *DIH Post-Install Configuration*

Chapter 3

Installation Procedures

Topics:

This section provides the procedures for DIH 1.x installation.

DIH Pre-Install Configuration

This section provides the procedures for DIH pre-install configuration.

Create Common Bulkconfig File

This procedure describes how to create the common DIH bulkconfig file on the PM&C server.

Create the bulkconfig file

a) Open a terminal window and log in to PM&C server as `root`.
b) Create the `/var/TKLC/smac/guest-dropin/bulkconfig` file.

Add DIH ISO images to the PM&C Image Repository

This procedure describes how to add DIH ISO files to the PM&C Image Repository.

Add the following ISO files to the PM&C Image Repository to be able to finish the DIH installation:

- TVOE
- TVOE guests TPD(s)
- Oracle
- IXP
- NSP
- WebLogic

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 NSP for pmacftpusr password.

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

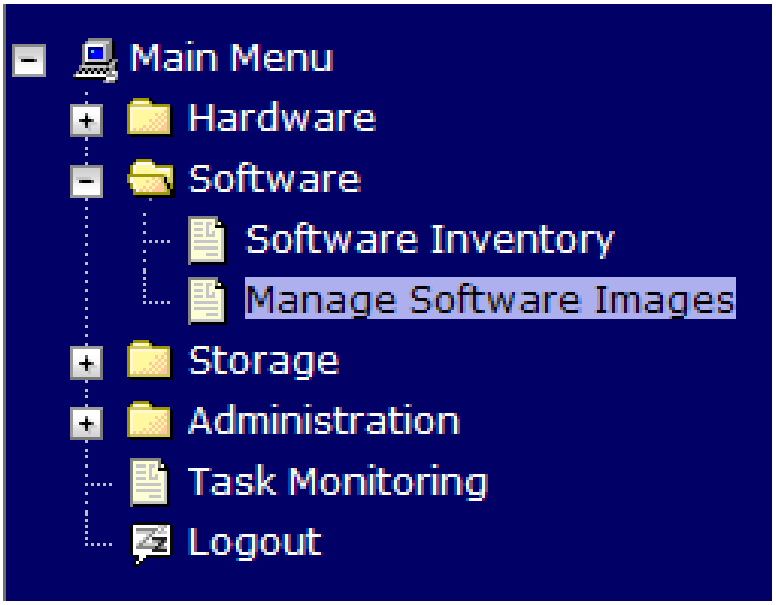
   Open web browser and enter:

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

   Login as pmacadmin user.

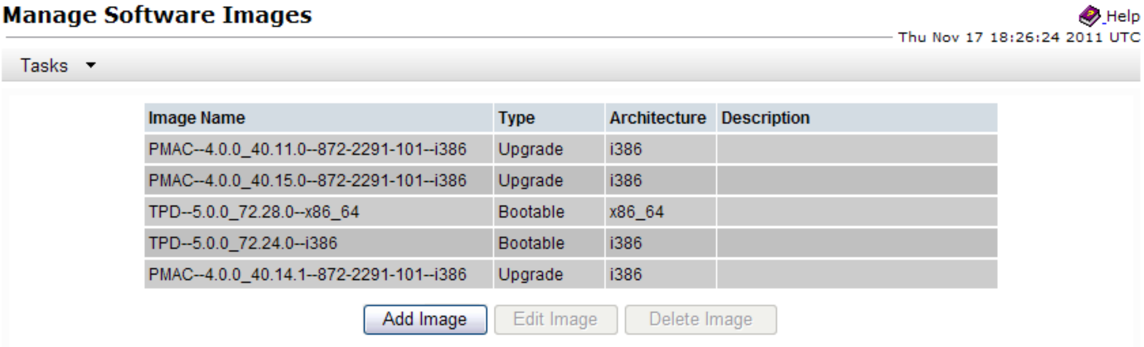
3. **PM&C GUI:** Navigate to Manage Software Images

   Navigate to **Main Menu ➤ Software ➤ Manage Software Images**



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

   Press the **Add Image** button .



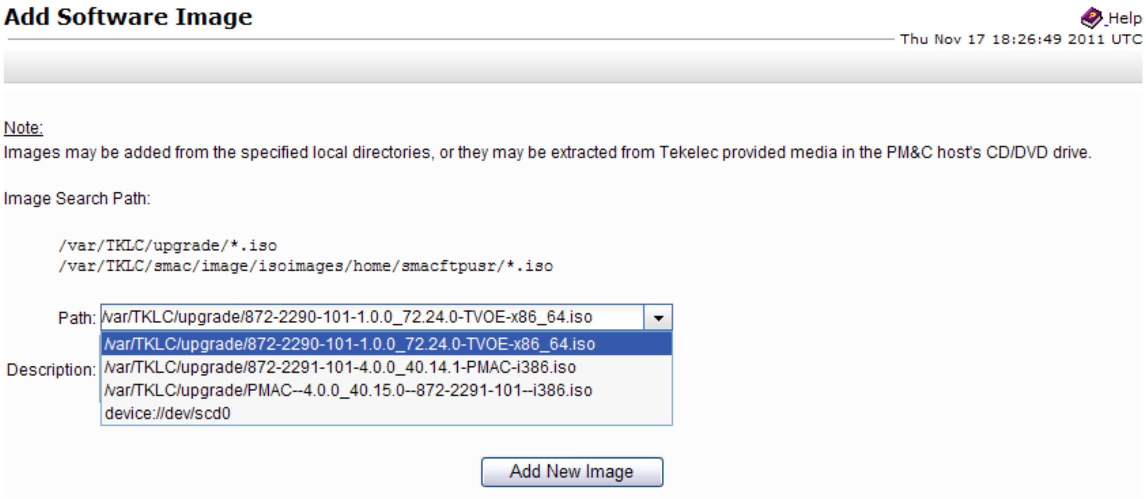
Manage Software Images

Thu Nov 17 18:26:24 2011 UTC

Image Name	Type	Architecture	Description
PMAC--4.0.0_40.11.0--872-2291-101--i386	Upgrade	i386	
PMAC--4.0.0_40.15.0--872-2291-101--i386	Upgrade	i386	
TPD--5.0.0_72.28.0--x86_64	Bootable	x86_64	
TPD--5.0.0_72.24.0--i386	Bootable	i386	
PMAC--4.0.0_40.14.1--872-2291-101--i386	Upgrade	i386	

5. **PM&C GUI:** Select an image

   Select an image to add, enter an appropriate image description and press the **Add New Image** button.



Add Software Image

Thu Nov 17 18:26:49 2011 UTC

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

Image Search Path:

```
/var/TKLC/upgrade/*.iso
/var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso
```

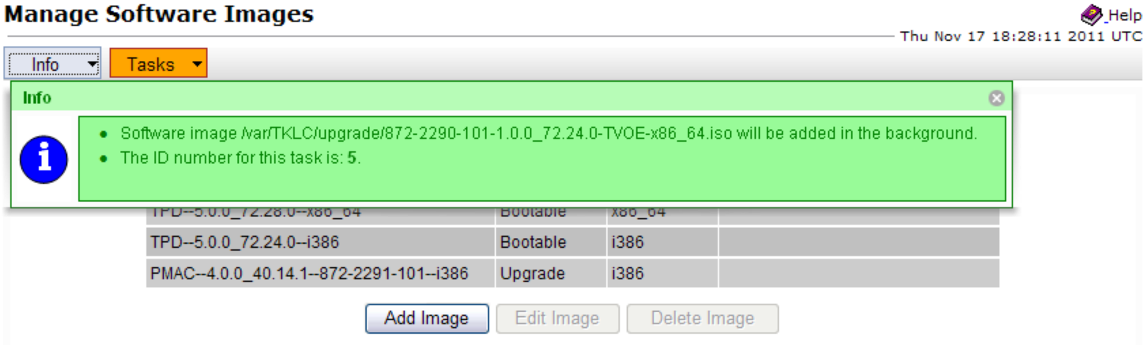
Path: /var/TKLC/upgrade/872-2290-101-1.0.0_72.24.0-TVOE-x86_64.iso

Description:

- /var/TKLC/upgrade/872-2290-101-1.0.0_72.24.0-TVOE-x86_64.iso
- /var/TKLC/upgrade/872-2291-101-4.0.0_40.14.1-PMAC-i386.iso
- /var/TKLC/upgrade/PMAC--4.0.0_40.15.0--872-2291-101--i386.iso
- device://dev/scd0

6. **PM&C GUI** Monitor the Add Image status

The `Manage Software Images` page is then redisplayed with a new background task entry in the table at the bottom of the page:



Manage Software Images

Thu Nov 17 18:28:11 2011 UTC

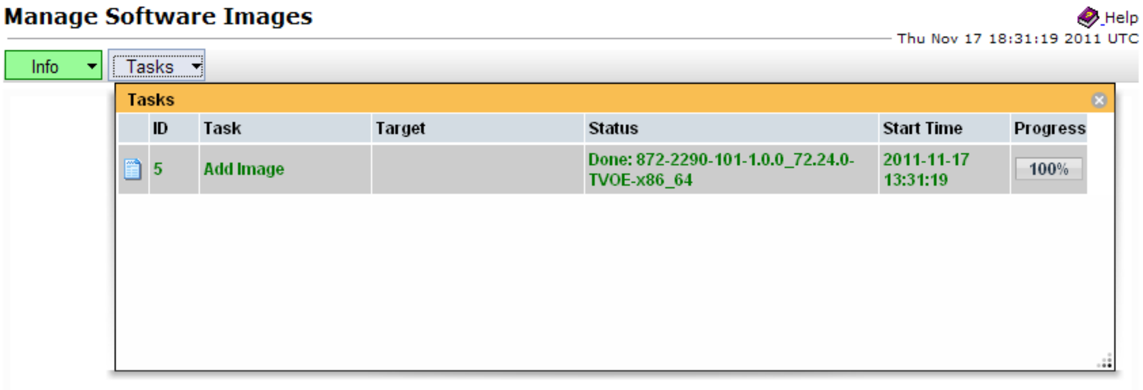
Info

- Software image /var/TKLC/upgrade/872-2290-101-1.0.0_72.24.0-TVOE-x86_64.iso will be added in the background.
- The ID number for this task is: 5.

TPD--5.0.0_72.28.0--x86_64	Bootable	x86_64	
TPD--5.0.0_72.24.0--i386	Bootable	i386	
PMAC--4.0.0_40.14.1--872-2291-101--i386	Upgrade	i386	

7. **PM&C GUI** Wait until the Add Image task finishes

When the task is complete, its text changes to green and its Progress column indicates "100%":



Manage Software Images

Thu Nov 17 18:31:19 2011 UTC

Tasks

	ID	Task	Target	Status	Start Time	Progress
	5	Add Image		Done: 872-2290-101-1.0.0_72.24.0-TVOE-x86_64	2011-11-17 13:31:19	100%

Install and Configure TVOE Host

This section provides the procedures for TVOE host installation and configuration.

Note: In case it is a previously installed system now being fresh installed, the disks need to be cleaned up. Therefore, go to the TVOE host and run this as root /usr/TKLC/plat/sbin/storageClean hpdisk --slot=3

Configure TVOE Host Performance (BIOS)

This section describes how to tune the performance settings for the TVOE host.

Note: Execute this section via iLO.

1. **Enter host server BIOS setup utility**
   a) Reboot the server
   b) As computer boots, press **F9** to access the BIOS setup utility and press **Enter**.
2. **Disable hyperthreading**
   a) Select **System Options** and press **Enter**.
   b) Select **Processor Options** and press **Enter**.
   c) Select **Intel Hyper threading Options** and press **Enter**.
   d) Select **Disable** and press **Enter**.
3. **Enable maximum performance**
   a) Select **Power Management Options** and press **Enter**.
   b) Select **HP Power Profile Options** and press **Enter**.
   c) Select **Maximum Performance** and press **Enter**.
4. **Exit BIOS**
   a) Press **Esc** to exit the utility.
   b) Press **F10** to confirm the exit from the utility.

Install Operating System on TVOE host

This procedure describes how to install the operating system on TVOE host.

Before you perform this procedure make sure the TVOE ISO has been added to the PM&C Image Repository. Then execute this procedure to install the Operating System (TVOE) on the TVOE host.

Note: Examples below shows the TPD operating system. The procedure is the same for the TVOE operating system.

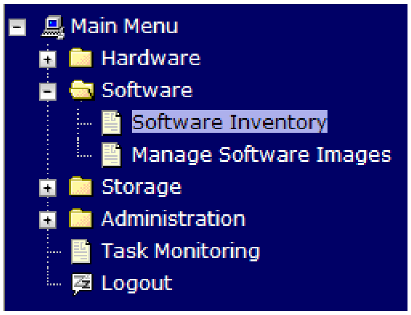
1. **PM&C GUI:** Login

   If needed, open web browser and enter:

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

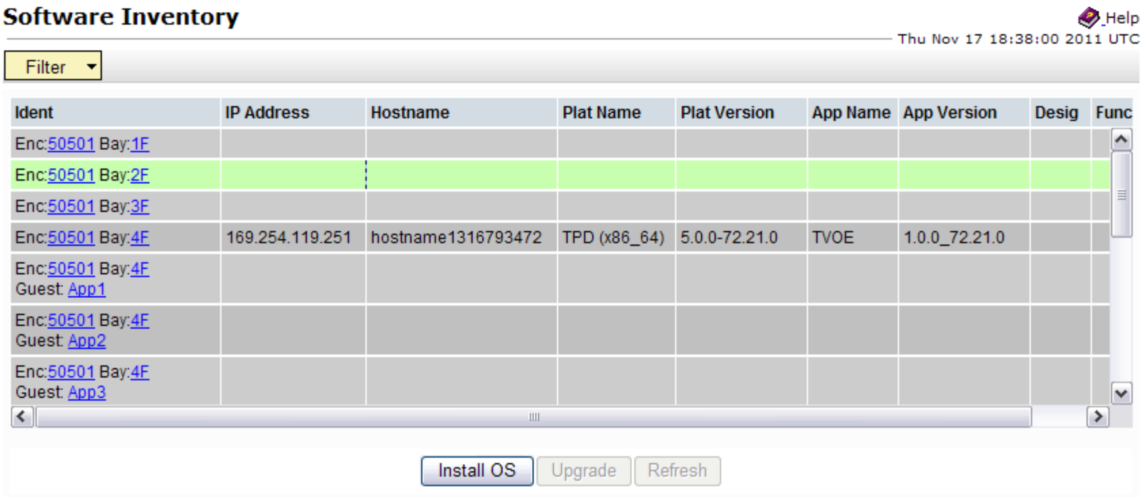
   Login as pmacadmin user.
2. **PM&C GUI:** Navigate to Software Inventory

Navigate to **Main Menu ➤ Software ➤ Software Inventory**.



3. **PM&C GUI:** Select servers

   Select the servers you want to IPM. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.



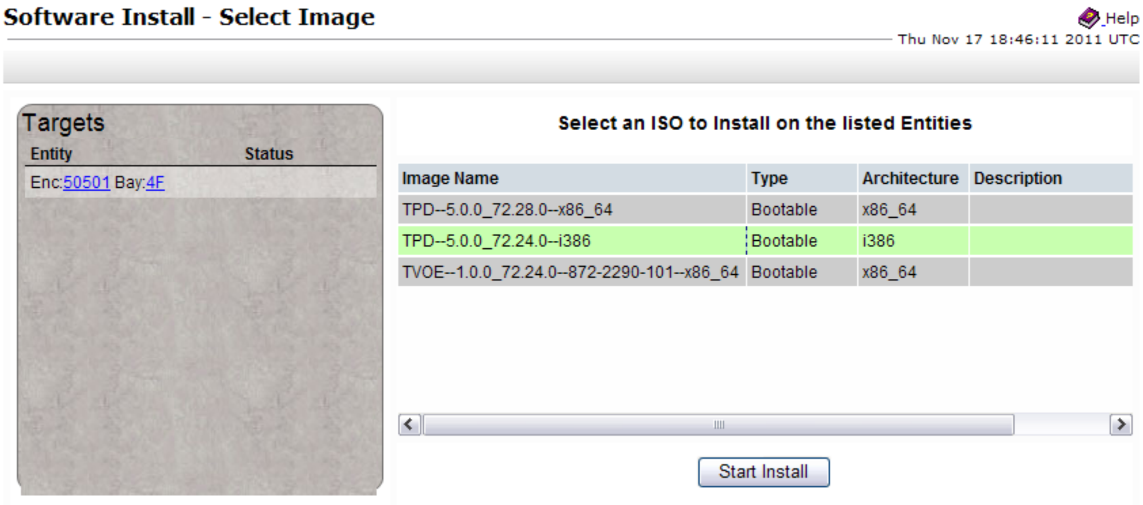
Thu Nov 17 18:38:00 2011 UTC

Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version	Desig	Func
Enc:50501 Bay:1F								
Enc:50501 Bay:2F								
Enc:50501 Bay:3F								
Enc:50501 Bay:4F	169.254.119.251	hostname1316793472	TPD (x86_64)	5.0.0-72.21.0	TVOE	1.0.0_72.21.0		
Enc:50501 Bay:4F Guest: App1								
Enc:50501 Bay:4F Guest: App2								
Enc:50501 Bay:4F Guest: App3								

   Then press the **Install OS** button.

4. **PM&C GUI:** Initiate OS Install

   The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.



Software Install - Select Image

Thu Nov 17 18:46:11 2011 UTC

Targets

Entity	Status
Enc:50501 Bay:4F	

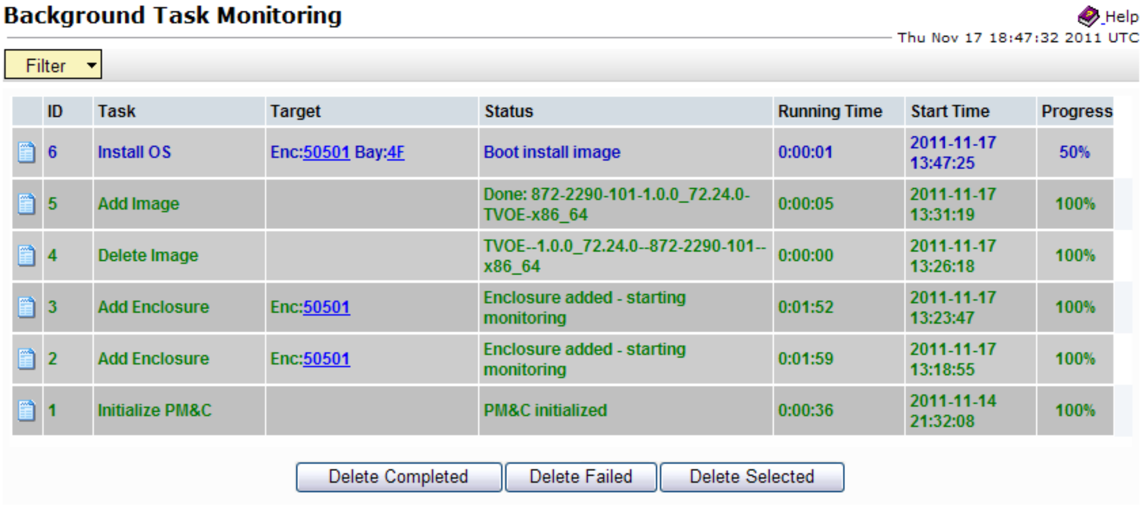
Select an ISO to Install on the listed Entities

Image Name	Type	Architecture	Description
TPD--5.0.0_72.28.0--x86_64	Bootable	x86_64	
TPD--5.0.0_72.24.0--i386	Bootable	i386	
TVOE--1.0.0_72.24.0--872-2290-101--x86_64	Bootable	x86_64	

Then press the **Start Install** button

5. **PM&C GUI:** Monitor OS Install

   Navigate to **Main Menu ➤ Task Monitoring** to monitor the progress of the OS Installation background task. A separate task will appear for each blade affected.



Background Task Monitoring

Thu Nov 17 18:47:32 2011 UTC

ID	Task	Target	Status	Running Time	Start Time	Progress
6	Install OS	Enc:50501 Bay:4F	Boot install image	0:00:01	2011-11-17 13:47:25	50%
5	Add Image		Done: 872-2290-101-1.0.0_72.24.0-TVOE-x86_64	0:00:05	2011-11-17 13:31:19	100%
4	Delete Image		TVOE--1.0.0_72.24.0--872-2290-101--x86_64	0:00:00	2011-11-17 13:26:18	100%
3	Add Enclosure	Enc:50501	Enclosure added - starting monitoring	0:01:52	2011-11-17 13:23:47	100%
2	Add Enclosure	Enc:50501	Enclosure added - starting monitoring	0:01:59	2011-11-17 13:18:55	100%
1	Initialize PM&C		PM&C initialized	0:00:36	2011-11-14 21:32:08	100%

When the task is complete, the task will change to green and the Progress column will indicate "100%".

Configure TVOE Host

This procedure describes how to configure the TVOE host.

Before you perform this procedure, make sure that the IXP ISO has been added to the PM&C Image Repository. Also make sure that the DIH common bulkconfig file is stored on `/var/TKLC/smac/guest-dropin/bulkconfig` and all information that the bulkconfig file contains is valid.

If the XMI network resides in bays other than 1 and 2 (bond0) then a bond1 interface needs to be created on TVOE server to get to the customer network. Refer to *Bond Creation* for further information.

1. **Obtain the control IP address of the TVOE host (PM&C GUI)**
   a) Open a web browser and log in to the PM&C NSP interface as `pmacadmin`.
   b) Navigate to **VM Management**.
   c) A **VM entities** list will appear. Click on particular TVOE host blade server (identified by `Enc:`*`id`* `Bay:`*`id`*).
   d) Navigate to **network** tab and note down the control network IP address of the TVOE host.
2. **Configure the TVOE host server hostname (TVOE iLO)**
   a) Open a web browser and log in to the TVOE host blade iLO.
   b) Open a virtual console and log in to the TVOE host blade as `root`.
   c) Navigate to platcfg. As `root` run:

   ```
   # su - platcfg
   ```

   d) Navigate to **Server Configuration ➤ Hostname**.
   e) Click **Edit** and enter the TVOE server hostname, the same that you previously set in the DIH Common Bulkconfig file. Save the changes and exit the platcfg menu.
3. **Configure SNMP on TVOE host**
   a) Connect on TVOE system as platcfg
   b) Go to **Network Configuration ➤ SNMP configuration ➤ NMS Configuration**.
   c) Add One Destination per guest.
      1. Select **Edit ➤ Add a new NMS server.**
      2. Enter IP (Internal IP of NSP server), port=162 and community=TEKELEC
      3. Select OK
   d) Confirm restart of Alarm Routing Service when exiting Edit.
   e) Exit
4. **Run TVOE bulk configuration (PM&C console)**
   a) Open a terminal window and log in to the PM&C server as `root`.
   b) Verify Designation and Function are set via the Platform configuration Menu before running the bulk configuration script. If it is not set please set Designation to 1A and Function to PMAC.
   c) Locate the directory where the imported IXP ISO is mounted. As `root` run:

   ```
   # ls -ld /usr/TKLC/smac/html/TPD/*IXP*
   ```

   locate the directory with the proper IXP version.
   d) Run the TVOE configuration using the `bulkConfig.pl` script from the IXP ISO. As `root` run:

   ```
   # /usr/TKLC/smac/html/TPD/IXP_version-IXP-i386/upgrade/lib/bulkConfig.pl --tvoe
    tvoe_host_control_ip -f /var/TKLC/smac/guest-dropin/bulkconfig
   ```

   where *IXP_version* is the version of the IXP NSP (from step 2b) and *tvoe_host_control_ip* is the TVOE control network IP address (from step 1d). Example:

   ```
   #
   /usr/TKLC/smac/html/TPD/872-2268-103-8.0.0_23.1.0-IXP-i386/upgrade/lib/bulkConfig.pl
    --tvoe 169.254.116.194  -f /var/TKLC/smac/guest-dropin/bulkconfig
   ```

   Note: The script will pause and expect the user to login to the TVOE host. Provide the root user id and password for the TVOE machine for the script to continue.

Create and Install Operating System on guest

This section provides the procedures to create and install operating system on TVOE guests.

Create Guests

This procedure describes how to create the guests on the TVOE host.

Before you perform this procedure, make sure that the IXP ISO has been added to the PM&C Image Repository. The IXP ISO contains the profile definitions for all DIH guest components. The guest profile names are following:

- `IXP` for IXP application
- `ora` for Oracle application
- `NSP` for NSP application
- `pmf`for PMF application
- `pmf`for Gen8 or Gen6 with Dual Port Ethernet Card
- `pmf-quad`Gen6 with Quad Port Ethernet Card
- `pmf-gen8`Gen8 Hardware with Quad Port Ethernet Card

1. **Navigate to VM entities list**
   a) Open a web browser and log in to the PM&C NSP interface as `pmacadmin`.
   b) Navigate to **VM Management**.
   c) A **VM entities** list will appear. Click on particular TVOE host blade server (identified by `Enc:`*`id`* `Bay:`*`id`*).
2. **Create guest**

   Note: Repeat this step for all 4 profiles (NSP, IXP, ora, pmf) to create 4 guests.

   a) Click on **Create Guest**.
   b) Click on **Import Profile**.
   c) Select the profile under the **ISO/profile** drop-down menu.
   d) Click on **Select Profile**.
   e) Click on **Create**. Monitor the progress of guest creation. Check that the guest has been created successfully.

Install the Operating System on Guests

This procedure describes how to install the operating system on the TVOE guests.

Before you perform this procedure, make sure you have all neccessary operating system (TPD) ISOs for all TVOE guests added in the PM&C Image Repository.

Note: Repeat this procedure for all 4 guests:

- `IXP`
- `ora`
- `NSP`
- `pmf`

Install TPD on guest

a) Open a web browser and log in to the PM&C NSP interface as `pmacadmin`.
b) Navigate to **VM Management**.
c) A **VM entities** list will appear. Click on particular TVOE host blade server (identified by `Enc:`*`id`* `Bay:`*`id`*).
d) A sublist with guests will appear. Click on a particular guest.
e) Click on **Install OS**. A list of available TPD ISOs will appear.
f) Select a particular TPD and click on **Start Install**.
g) Observe **Task Monitoring** page for installation progress. Wait until the operation system is installed. Check status that the operation system has been installed successfully.

Install Oracle Guest

This section provides the procedures for incremental upgrade of the DIH applications running on the TVOE guest. The Oracle Guest is not included in chapter 5 as it does not require upgrade.

Install Oracle Guest

This procedure describes how to install the Oracle NSP on the Oracle guest

Before you perform this procedure, make sure you have all neccessary operating system (TPD) ISOs for all TVOE guests added in the PM&C Image Repository.

Before you perform this procedure, make sure the Oracle ISO has been added to the PM&C Image Repository.

1. **Get guest's control network IP address**

a) Open a terminal window and log in to the TVOE host as `root`.
b) List all available guests. As `root` run:

```
# virsh list
```

example:

```
[root@opica ~]# virsh list
 Id Name                 State
----------------------------------
 17 IXP            running
 26 ora            running
 38 NSP            running
 42 pmf            running
```

c) Connect to the serial console of guest. As `root` run:

```
# virsh console guest_name
```

where *guest_name* is the name of the guest. Example:

```
[root@opica ~]# virsh console IXP
Connected to domain IXP
Escape character is ^]
```

Press `<enter>` to get to login prompt of the guest. Login as `root`.

d) Get control network IP address. As `root` run:

```
# ifconfig control
```

and note down the IP address of control network.

2. **Login to Oracle guest and set hostname**

   Note: You must set the same hostname as you have in the DIH common bulkconfig file.

   a) Open a terminal window and log in to the Oracle guest as `root` using the control network IP address.
   b) Enter the platcfg menu. As `root` run:

   ```
   # su - platcfg
   ```

   c) Navigate to **Server Configuration** ➤ **Hostname**. Click **Edit** and set the server hostname. Exit the platcfg menu.

3. **Install Oracle from PM&C GUI**

   Note: The following steps describes how to install the Oracle to Oracle guest using PM&C install/upgrade NSP.

   a) Open a web browser and log in to the PM&C NSP interface as `pmacadmin`.
   b) Navigate to **VM Management**.
   c) A **VM entities** list will appear. Click on particular TVOE host blade server (identified by `Enc:`*`id`* `Bay:`*`id`*).
   d) A sublist with guests will appear. Click on a particular guest.
   e) Click on **Upgrade**. A list of available ISOs will appear.
   f) Select a particular NSP ISO and click on **Start Upgrade**. An NSP upgrade will be triggered.
   g) Observer **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Check status that the NSP has been upgraded successfully.

4. **Configure Oracle**

   a) Log back to rebooted guest as `root`.
   b) Configure Oracle. As `root` run:

   ```
   # /opt/dih/configureOracle.sh
   ```

   wait until the Oracle configuration will finish.

Install IXP Guest

This section provides the procedures for installing the IXP on the IXP guest.

Install IXP Guest

This procedure describes how to install the IXP NSP on IXP guest.

Before you perform this procedure, make sure the IXP ISO has been added to the PM&C Image Repository.

1. **Get guest's control network IP address**

   a) Open a terminal window and log in to the TVOE host as `root`.
   b) List all available guests. As `root` run:

   ```
   # virsh list
   ```

example:

```
[root@opica ~]# virsh list
 Id Name                 State
----------------------------------
 17 ixp                  running
 26 ora                  running
 38 nsp                  running
 42 pmf                  running
```

c) Connect to the serial console of guest. As `root` run:

```
# virsh console guest_name
```

where *guest_name* is the name of the guest. Example:

```
[root@opica ~]# virsh console ixp
Connected to domain ixp
Escape character is ^]
```

Press `<enter>` to get to login prompt of the guest. Login as `root`.

d) Get control network IP address. As `root` run:

```
# ifconfig control
```

and note down the IP address of control network.

2. Login to IXP guest and set hostname

Note: You must set the same hostname as you have in the DIH common bulkconfig file.

a) Open a terminal window and log in to the IXP guest as `root` using the control network IP address.

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

```
# su - platcfg
```

c) Navigate to **Server Configuration ➤ Hostname**. Click **Edit** and set the server hostname. Exit the platcfg menu.

3. Install IXP from the PM&C GUI

Note: The following steps describes how to install the IXP application to IXP guest using PM&C install/upgrade NSP.

a) Open a web browser and log in to the PM&C NSP interface as `pmacadmin`.

b) Navigate to **VM Management**.

c) A **VM entities** list will appear. Click on particular TVOE host blade server (identified by `Enc:`*`id`* `Bay:`*`id`*).

d) A sublist with guests will appear. Click on a particular guest.

e) Click on **Upgrade**. A list of available ISOs will appear.

f) Select a particular NSP ISO and click on **Start Upgrade**. An NSP upgrade will be triggered.

g) Observer **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Check status that the NSP has been upgraded successfully.

4. Finalize IXP guest installation

Note: Before you execute this step, verify that Oracle guest is up and running.

a) Wait until IXP will reboot. Than log in to the IXP guest as `root`. As `root` run:

```
# installIXP
```

Wait until installation finishes. Check there are no errors.

Post-install Oracle Configuration

This procedure describes how to run the automatic Oracle post-install script. This procedure allocates necessary data and index files and runs various Oracle post-install settings and tunings.

This procedure is applicable to DIH IXP PDU Storage server. This procedure will run post-install configuration on DIH Oracle server for IXP purpose.

1. Open a terminal window and log in to DIH IXP PDU Storage server as `root`.
2. Run DIH Oracle configuration. As `root` run:

   ```
   # cd_oracle_utils
   # ./oracle-postinstall.pl -auto -conn=system/manager@ixp_oracle/pic
   -connsys=sys/oracle@ixp_oracle/pic
   ```

3. When the script finishes, check the log file `/var/TKLC/log/ixp/postinstall-oracle.log` for any errors.

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

   Example output:

   ```
   --CUT--
   inf | --- Calculated new sizing in space usage:
   inf |                  part |    existing |    requested | target
   inf |             Temp size | 12884901888 |  17179869184 | as requested
   inf |         DATA_CDR size |137438953472 |1272487125741 | 1271310319616
   inf |         DATA_IND size | 34359738368 |1040365377590 | 1030792151040
   inf |oraindex DATA_CDR size |           0 | 289237746768 | 274877906944
   inf | --- Calculated new sizing in number of files:
   inf |                  part |  exists |requested|  create | cdr:ind %
   inf |            Temp files |       6 |       8 |       2 |       na
   inf |         DATA_CDR data |       8 |      74 |      66 |  48.879
   inf |         DATA_IND data |       2 |      60 |      58 |  39.632
   inf |oraindex DATA_CDR data |       0 |      16 |      16 |  10.569
   war | Will create 2 temp files.
   war | Will create 66 DATA_CDR data files.
   war | Will create 58 DATA_IND data files.
   war | Will create 16 DATA_CDR data files at oraindex.
   inf | File:   0/142 at 1GB avg 0.00s, ETA    0.00s
   inf | File:   1/142 at 1GB avg 0.00s, ETA    0.00s
   inf | File:   2/142 at 1GB avg 0.00s, ETA    0.00s
   inf | File:   3/142 at 1GB avg 3.69s, ETA 8201.00s
   inf | File:   4/142 at 1GB avg 3.69s, ETA 8145.94s
   inf | File:   5/142 at 1GB avg 3.70s, ETA 8111.01s
   inf | File:   6/142 at 1GB avg 3.70s, ETA 8057.48s
   inf | File:   7/142 at 1GB avg 3.71s, ETA 8014.10s
   inf | File:   8/142 at 1GB avg 3.72s, ETA 7969.14s
   --CUT--
   ```

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.

Install NSP Guest

This section provides the procedures for installing the NSP on the NSP guest.

Install NSP Guest

This procedure describes how to install the NSP application on NSP guest.

Before you perform this procedure, make sure the NSP and WebLogic ISOs has been added to the PM&C Image Repository.

Note: Oracle guest must be already up and running

1. **Get guest's control network IP address**

a) Open a terminal window and log in to the TVOE host as `root`.

b) List all available guests. As `root` run:

```
# virsh list
```

example:

```
[root@opica ~]# virsh list
 Id Name                 State
----------------------------------
 17 ixp                  running
 26 ora                  running
 38 nsp                  running
 42 pmf                  running
```

c) Connect to the serial console of guest. As `root` run:

```
# virsh console guest_name
```

where *guest_name* is the name of the guest. Example:

```
[root@opica ~]# virsh console ixp
Connected to domain ixp
Escape character is ^]
```

Press `<enter>` to get to login prompt of the guest. Login as `root`.

d) Get control network IP address. As `root` run:

```
# ifconfig control
```

and note down the IP address of control network.

2. **Login to the NSP guest and set hostname.**

   Note: You must set the same hostname as you have in the DIH common bulkconfig file.

   a) Open a terminal window and log in to the NSP guest as `root` using the control network IP address.

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

   ```
   # su - platcfg
   ```

   c) Navigate to **Server Configuration ➤ Hostname**. Click **Edit** and set the server hostname. Exit the platcfg menu.

3. **Install WebLogic from the PM&C GUI**

   Note: The following steps describes how to install the WebLogic application to the Application guest using PM&C install/upgrade application.

   a) Open a web browser and log in to the PM&C application interface as `pmacadmin`.

   b) Navigate to **VM Management**.

   c) A **VM entities** list will appear. Click on particular TVOE host blade server (identified by `Enc:`*`id`* `Bay:`*`id`*).

   d) A sublist with guests will appear. Click on a particular guest.

   e) Click on **Upgrade**. A list of available ISOs will appear.

   f) Select a particular application ISO and click on **Start Upgrade**. An application upgrade will be triggered.

   g) Observer **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Check status that the application has been upgraded successfully.

4. **Install NSP application on NSP guest**

Note: This step describes how to install the Application on the Application guest. Execute this procedure from Application guest console.

a) Open a terminal window and log in to the NSP guest as `root` using the control network IP address.
b) Download the NSP ISO from the PM&C to `/var/TKLC/upgrade` directory. The image can be found on the PM&C in /var/TKLC/smac/image
c) Enter the platcfg menu. As `root` run:

```
# su - platcfg
```

d) Trigger the NSP application installation. Navigate to **Maintenance ➤ Upgrade ➤ Initiate Upgrade** to trigger the upgrade. Wait until the upgrade finishes. During the installation you may be prompted for `root` password. Enter if requested.

Configure Node A and Restart NTP

This procedure describes how to install Node A after NSP has been installed. Node A RPMs from xMF are necessary for various NSP application functions (for example, ProDiag and ProMonitor).

Before you perform this procedure:

- The NSP One-box or Primary server must be installed.
- Make sure the xMF DVD/CD or ISO file is available on the same TPD platform as the NSP. To verify, run the `getPlatRev` command.

1. **Install Node A**

a) Insert the xMF DVD/CD or copy the xMF ISO file to the NSP server.
b) Log in as `root` on the NSP server and run:

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

When prompted for the ISO file, provide the complete ISO path. For example:

```
/var/TKLC/upgrade/iso_name.iso
```

where *iso_name.iso* is the name of the ISO file.

A confirmation prompt appears.

c) Enter **Yes** to confirm.

Note: You do not need to reboot the server.

2. **Restart the NTP**

Log in as `root` on the NSP server and run:

```
# service ntpd restart
```

3. **Analyze the installation log and run healtheck script**

a) Check the Node A installation log (`/var/TKLC/log/upgrade/nodeA_install.log`). If there are any errors in the log, contact Tekelec Customer Care Center.
b) Run healthcheck script to verify the Node A state. Log in as `cfguser` on NSP server and run:

```
S analyze_server.sh -p
```

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:

```
NSP0801-PW:/export/home/cfguser analyze_server.sh -p
07:41:14: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
07:41:14: date: 05-16-11, hostname: NSP0801-PW
07:41:14: TPD VERSION: 4.2.3-70.86.0
07:41:14: XMF VERSION: [ 70.1.0-30.1.0 ]
07:41:14: -------------------------------------------------
07:41:14: Checking disk free space
07:41:14: No disk space issues found
07:41:14: Checking syscheck - this can take a while
07:41:19: No errors in syscheck modules
07:41:19: Checking statefiles
07:41:19: Statefiles do not exist
07:41:19: Checking runlevel
07:41:19: Runlevel is OK (N 4)
07:41:19: Checking upgrade log
07:41:20: Install logs are free of errors
07:41:20: Analyzing IDB state
07:41:20: IDB in START state
07:41:20: Checking IDB database
07:41:20: iaudit has not found any errors
07:41:20: Analyzing processes
07:41:20: Processes analysis done
07:41:20: All tests passed. Good job!
07:41:20: 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
...
909-2122-001 Revision 1, April 22, 2011 133
xMF Application Installation Procedures08:18:35: >>> Error: 1 test(s) failed!
08:18:35: ENDING HEALTHCHECK PROCEDURE WITH CODE 2
```

Note: Ignore the error about the run state 'X' instead of 'A' since no server is defined yet. The state will become 'A' after a 5 minute timeout.

Configure Purchased Tokens

This procedure describes how to configure purchased tokens after NSP is installed.

During initial install, the default value for the number of tokens is `0`, which means that no one will be able to login.

1. Open a web browser and log in as `TklcSrv` on the NSP application interface.

   Note: On the first Login `TklcSrv` user is prompted to change his password.

   The window will appear.

   Fill in the `Old Password` (default password), `New Password` (enter `Tekelec1$`) and `Confirm Password` (enter `Tekelec1$`) fields. Click **OK**.
2. Select the **Security** application.
3. Select **Action ➤ Manage Tokens**.
   The **Tokens** window appears.

4. Type the appropriate value (a value greater than zero, e.g., `5`) in the **Purchased token** field and click **Apply**.

Verify NSP Application Documentation

This procedure describes how to verify that the NSP documentation is installed.

Note: The Application documents are automatically installed when the Application application is installed.

1. Log in to the NSP application interface.
2. Select **Help ➤ Users Manual**.
   The Index page for that application opens.

It is recommended that each application is tested in this manner. In addition, test the PDF link to check that the printable PDF file opens.

NSP Post-Install Healthcheck

This procedure describes how to run various healthchecks and tests on the NSP server after the NSP application has been installed.

1. Open a terminal window and log in as `root` on the NSP server.
2. As `root`, run:

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

   Note: If the `NOT OK` message appears anywhere in the output, contact the Tekelec Customer Care Center.

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

   Verify the following:

   - Port 80 connectivity is **OK**
   - Oracle server health is **OK**
   - WebLogic health for ports 5556, 7001, 8001 is **OK**
   - Oracle em console connectivity is **OK**
   - The disk partition includes the following lines, depending on whether rackmount , blades or DIH setup:
     - If rackmount, the output contains the following lines:

       ```
       /dev/cciss/c1d1p1     275G  4.2G  271G   2% /usr/TKLC/oracle/ctrl1
       /dev/cciss/c1d0p1     825G   34G  792G   5% /usr/TKLC/oracle/oradata
       /dev/cciss/c1d2p1     275G   16G  260G   6% /usr/TKLC/oracle/backup
       ```

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

     - If blades, output contains following lines:

       ```
       /dev/mapper/nsp_redo_vol    69G  4.2G  65G   7%  /usr/TKLC/oracle/ctrl1
       /dev/mapper/nsp_data_vol    413G 8.3G  405G  2%  /usr/TKLC/oracle/oradata
       /dev/mapper/nsp_backup_vol  138G 30G   108G  22% /usr/TKLC/oracle/backup
       ```

- In case of DIH setup, output contains following lines:

```
/dev/vdb        99G  652M  93G  1%  /usr/TKLC/oracle/backup
```

Install PMF Guest

This section provides the procedures for installing the PMF on the PMF guest.

Install PMF guest

This procedure describes how to install the PMF application on the PMF guest.

Before you perform this procedure, make sure you have all neccessary operating system (TPD) ISOs for all TVOE guests added in the PM&C Image Repository.

Before you perform this procedure, make sure that PMF ISO has been added to PM&C Image Repository.

1. **Get guest's control network IP address**

   a) Open a terminal window and log in to the TVOE host as `root`.

   b) List all available guests. As `root` run:

   ```
   # virsh list
   ```

   example:

   ```
   [root@opica ~]# virsh list
    Id Name                 State
   ----------------------------------
    17 ixp                  running
    26 ora                  running
    38 nsp                  running
    42 pmf                  running
   ```

   c) Connect to the serial console of guest. As `root` run:

   ```
   # virsh console guest_name
   ```

   where *guest_name* is the name of the guest. Example:

   ```
   [root@opica ~]# virsh console ixp
   Connected to domain ixp
   Escape character is ^]
   ```

   Press `<enter>` to get to login prompt of the guest. Login as `root`.

   d) Get control network IP address. As `root` run:

   ```
   # ifconfig control
   ```

   and note down the IP address of control network.

2. **Install PMF from PM&C GUI**

   Note: The following steps describes how to install the PMF application to PMF guest using PM&C install/upgrade application.

   a) Open a web browser and log in to the PM&C application interface as `pmacadmin`.

b) Navigate to **VM Management**.

c) A **VM entities** list will appear. Click on particular TVOE host blade server (identified by `Enc:`*`id`* `Bay:`*`id`*).

d) A sublist with guests will appear. Click on a particular guest.

e) Click on **Upgrade**. A list of available ISOs will appear.

f) Select a particular application ISO and click on **Start Upgrade**. An application upgrade will be triggered.

g) Observer **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Check status that the application has been upgraded successfully.

IMI Address Configuration

Perform this task, only if the DIH addresses were changed to the IMI addresses in the *Create External Bulkconfig File*

1. netAdm set-address=x.x.x.x-netmask=255.255.255.x-device=pic
2. Navigate to **Network Configuration ➤ Modify Hosts File**. Click Edit and Delete Host.
3. Select cust0-a entry
   a) Click Yes
4. Select Delete Host
5. Select appserver entry
   a) Click Yes
6. Select Delete Host
7. Select ntpserver1 entry
   a) Click Yes
8. Select Add Host
   a) x.x.x.x (IMI pmf-0a IP address)
   b) cust-0a
   c) Click Yes
9. Select Add Host
   a) x.x.x.x (IMI nsp IP address)
   b) appserver
   c) Click Yes
10. Select Add Host
    a) x.x.x.x (IMI tvoe address)
    b) ntpserver1
    c) Click Yes
11. Select Add Alias
    a) Select cust-0a
    b) Enter new alias: pmf-0a
12. Exit the platcfg menu
13. #su - cfguser-c" prod.start-C
14. #reboot

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
   ```

   Note: Ignore the error about the run state 'X' instead of 'A' since no server is defined yet. The state will become 'A' after a 5 minute timeout.

DIH Post-Install Configuration

This section provides the procedures for DIH post-installation configuration.

Configure Site and Subsystem for xMF

This procedure describes how to create a site on NSP and set a subsystem in this new site.

The subsystem is treated by DIH as a cluster, accessible by NSP through this IP address.

A dedicated IP address, called Virtual IP (VIP), is needed for the subsystem. This address must be a real address in the subsystem subnet that is not physically used by any other server or equipment. The current Active Master server in the subsystem is the server representing the VIP.

For a standalone PMF, the VIP is the IP address of the PMF server. For a single-server IMF, it is possible to assign the server IP address as VIP; however, when additional servers are added, the VIP address must be changed to a dedicated IP address to work properly. It is recommended that a dedicated IP address be used from the beginning, to avoid changing the VIP when more servers are added.

Note: There is only one xMF subsystem supported per site. If a standalone PMF is in a site/subsystem, no other IMF or PMF subsystem or standalone PMF can be added. They need to be added to different logical site in **Centralized Configuration**. All of the configuration is performed through the NSP application interface.

1. **Log in to the NSP application**
   a) Log in as user "**tekelec**" to the NSP application interface using the NSP IP address.
   a) Click **Centralized configuration**.

   The NSP application launches.
2. **Create a site on NSP**
   a) Select **Equipment Registry ➤ Sites ➤ Add**.
   b) Type the desired site name and click **Add**.
3. **Add the server(s) on NSP**

   Note: Skip this step if the Site already exists.

   a) Select **Equipment Registry ➤ Sites ➤** ***New site name created*** **➤ XMF ➤ Add**
   b) Type the server IP address(es) for the xMF subsystem into both the IP Address and VIP address fields and click **Add**. In the popup that is displayed, accept the reuse of the IP address.

   Note: Use the command # **ifconfig pic** from the terminal to get the IP address.

   c) Click **Create**.
4. **Apply the changes on NSP**
   a) Select **Acquisition ➤ Sites ➤** *New site name created*
   b) Expand the subsystem; then, right-click on embedded subsytem name and select **Apply changes**.
   c) Click **Next** to see warnings.
   d) Click **Apply Changes**.
   e) Click **Yes** to confirm the change.

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!
```

Configure IXP

This procedure describes how to configure IXP server.

This procedure is applicable to IXP DIH server.

Adjust IXP server

a) Log in to the IXP DIH server as `root`.

b) As `root` run:

```
bc_adjust_subsystem.sh
```

Wait until server reconfigures and check for any errors. You may be prompted for `root` and `cfguser` password. Enter them if asked.

Add IXP Subsystem to CCM

This procedure describes how to add the DIH IXP subsystem to the CCM on NSP.

This procedure is performed through the NSP application interface.

1. **Log in to the NSP and open Centralized Configuration (CCM)**

   a) Log in to the NSP application interface using the NSP Primary server IP address.

   Note: Use the command # **ifconfig pic** from the terminal to get the IP address.

   b) Open the **Centralized Configuration** application.

   c) Select **Equipment Registry**.

2. **Configure the new site**

   a) Right-click the **Sites** list and select **Add** to enter new site configuration.

   b) Type the **Site name** and **Description** and click **Add**.

3. **Add the IXP subsystem to the site**

   a) Navigate to **Sites**.

   b) Twice right-click **IXP** and select **Add** to enter the IXP subsystem configuration.

   c) Type values for the following fields:

   - For the **Subsystem Name** field use the IXP hostname defined in the bulkconfig file. Exclude the designation i.e.1a. For example: ixp0002.
   - For the **VIP Address** field use the DIH address defined in the bulkconfig file for the IXP.

- For the **Storage field**, select the desired XDR storage. If adding the second enclosure IXP of a dual-enclosure setup, choose for the **Storage** field DIH_IXP_STORAGE_ENC2 (or named storage created earlier).
- For the **IP Address** field use the DIH address defined in the bulkconfig file for the IXP. This is the same address used in the VIP Address field.

Note: For DIH use as Virtual IP the internal network IP of IXP server (pic interface in the /root/bulkconfig file).

d) Click **Add**.

e) Verify that the server is listed in the **Locations** list.

f) Click **Create**.
Information is synchronized from the IXP servers to the NSP.

g) Verify that there are no errors on the result page that will display. If there are any errors contact the Tekelec Customer Care Center.

4. Apply the configuration to the IXP subsystem

a) Navigate to **IXP ➤ Sites**.

b) Open **IXP**.

c) Right-click the subsystem and select **Apply changes**.

d) Click**Next**.

e) Click **Apply changes** .

f) Verify that there are no errors on the result page that will display. If there are any errors contact the Tekelec Customer Care Center.

IXP Subsystem Healthcheck

This procedure describes how to run the automatic healthcheck of the IXP guest. This healthcheck also checks the Oracle guest has started as in operational state.

1. Open a terminal window and log in on any IXP server in the IXP subsystem you want to analyze.
2. As `cfguser`, run:

```
$ analyze_subsystem.sh
```

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

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

Example of overall output:

```
[cfguser@ixp2222-1a ~]$ analyze_subsystem.sh
-----------------------------------------------------
ANALYSIS OF SERVER ixp2222-1a STARTED
-----------------------------------------------------
10:16:05: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
10:16:05: date: 05-20-11, hostname: ixp2222-1a
10:16:05: TPD VERSION: 4.2.3-70.86.0
10:16:05: IXP VERSION: [ 7.1.0-54.1.0 ]
10:16:05: XDR BUILDERS VERSION: [ 7.1.0-36.1.0 ]
10:16:05: ---------------------------------------------
```

```
10:16:05: Analyzing server record in /etc/hosts
10:16:05:       Server ixp2222-1b properly reflected in /etc/hosts file
10:16:05: Analyzing IDB state
10:16:05:       IDB in START state
...
12:21:48: Analyzing disk usage
...
10:24:09: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp2222-1b

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

Example of a successful test:

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

Example of a failed test:

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

3. Run Oracle guest healthcheck.

a) Open a terminal window and log in to Oracle guest as `grid` user.

b) As `grid` run:

```
$ crsctl status resource -t
```

c) Once the Oracle stack has fully started, the output should be as follows where the STATE_DETAILS of the database resource (ora.pic.db) equals "Open".

```
---------------------------------------Open-----------------------------
NAME          TARGET  STATE        SERVER                  STATE_DETAILS
-----------------------------------------------------------------------------
Local Resources
-----------------------------------------------------------------------------
ora.DATA.dg
              ONLINE  ONLINE      ora
ora.LISTENERASM.lsnr
              ONLINE  ONLINE      ora
ora.asm
              ONLINE  ONLINE      ora                      Started
ora.ons
              ONLINE  ONLINE      ora
-----------------------------------------------------------------------------
Cluster Resources
-----------------------------------------------------------------------------
ora.cssd
      1        ONLINE  ONLINE      ora
ora.diskmon
      1        ONLINE  ONLINE      ora
ora.evmd
      1        ONLINE  ONLINE      ora
ora.pic.db
      1        ONLINE  ONLINE      ora                      Open
```

License DataFeed Host Server on NSP

This procedure describes how to license the DataFeed host server on the NSP.

This procedure is performed on the NSP Primary server.

For an estimated time for this procedure, refer to the IXP flowchart.

1. **Log in on the NSP Primary server and list the available hosts**
   a) Open a terminal window and log in as `tekelec` on the NSP Primary WebLogic server.
   b) List the available hosts and already licensed hosts.

   As `tekelec`, run:

   ```
   $ cd /opt/nsp/scripts/datafeed
   $ ./listLicencedHosts
   ```

   Example output:

   ```
   *** Available hosts ***
   Host id=528 ip address=10.0.0.10
   Host id=13881 ip address=10.0.0.11
   Host id=363 ip address=localhost
   Host id=357 ip address=192.168.1.10
   Host id=21255 ip address=192.168.1.11
   *** Licenced hosts ***
   Host id=528 ip address=10.0.0.10
   Host id=13881 ip address=10.0.0.11
   ```

   c) Make a list of the IXP IDs of all hosts that you want to license and those that have not been licensed yet.
2. **License DataFeed host**

   As `tekelec`, run:

   ```
   $ ./licenceHost hostID
   ```

   where *hostID* is the host ID of the DataFeed host that was provided as a result of the previous step `./listLicencedHosts` command.

   Example output:

   ```
   [tekelec@nsp scripts]# ./licenceHost 357
   * Host with HOST_ID=357 was successfully licenced
   ```

Configure JmxAgent

This procedure describes how to configure the JmxAgent to allow HTTP access.

1. Open a terminal window and log in as `cfguser` on the IXP server.
2. Edit `/opt/TKLCjmxagent/in/agent.properties`
3. Change `HttpAdaptor=false` to `HttpAdaptor=true`
4. Save changes
5. Restart JmxAgent by command:

   ```
   # pm.kill JmxAgent
   ```

Install xDR Builders

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

1. **Log in on the NSP Primary server and insert the xDR DVD/CD or copy the ISO file**
   a) Open a terminal window and log in on the NSP Primary WebLogic server.
   b) Insert the xDR Builders DVD/CD or copy the xDR Builder ISO file to the NSP Primary WebLogic server.

2. **Run the install script**
   a) As `root`, run:

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

   The following prompt appears:

   ```
   Please enter path to Builder CDROM or ISO [/media/cdrom]
   ```

   Note: This step may ask for the root password multiple times.

   b) Enter the appropriate response based on the media used:

   - For a DVD/CD, press **Enter**.
   - For an ISO file, enter the exact path including the ISO file name.

   c) Wait until the installation is complete.

3. **Verify the ISO installation on NSP**
   a) Open a web browser and log in as `TklcSrv` on the NSP application interface.
   b) Open the **Upgrade Utility**.
   c) Click **Manage Builder Rpm** in the left tree.

   A list of xDR Builder RPMs appears. The ISO file installed in the previous step is on this list, with a state **Not Uploaded**.

4. **Upload Builders RPM**
   a) Select the desired xDR Builder RPM with the **Not Uploaded** state and click **Upload**.
   A confirmation window appears.
   b) Click **Continue** to continue the RPM upload.
   If the upload is successful, then the RPM state changes to **Uploaded**. If the upload fail contact the Tekelec Customer Care Center.

5. **Associate the xDR Builders RPM with the IXP subsystem**
   a) Click **View Builder RPM Status** in the left tree.
   A list of the IXP subsystems appears.
   b) Select one or more IXP subsystems and click **Associate RPM Package**.

   A list of Builder RPMs that are uploaded in NSP appears.

   c) Select the appropriate xDR Builder RPM and click **Associate**.
   If the association is successful, then the list of the subsystems is updated. The **RPM Name** column contains the new RPM package name and **Association Status** is marked as **OK**. If the association fails contact the Tekelec Customer Care Center.

6. **Apply the configuration to the IXP subsystem**

a) Return to the main page of the NSP application interface.
b) Open the **Centralized Configuration** application.
c) Navigate to **IXP**.
d) Open **Sites** and open the site; then, open **IXP**.
e) Right-click the subsystem and select **Apply changes…**.
f) Click **Next**.
g) Click **Apply Changes**.
h) When change is complete, verify there are no errors on the result page.

7. **Install the xDR Builders RPM on IXP**

a) Return to the main page of the NSP application interface.
b) Open the **Upgrade Utility**.
c) Click **View Builder RPM Status** in the left tree.

The available IXP subsystems with their respective RPM **Associate Status** and **Install Status** appears.

d) Before initiating the builder installation, make sure the **Builder RPM** that you want to install on the IXP subsystem is associated with the IXP subsystem as indicated by **RPM Name** column and **Association Status** marked as **OK**. Also, **Install Status** should contain either **-** or **Not Started**.
e) Select one or more IXP subsystems and click **Install RPM Package**.
If the installation is successful, the **Install status** changes to **OK**. If the installation fails contact the Tekelec Customer Care Center.

xDR Builders Licensing

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

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

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.

Configure NSP FTP or SFTP Server

This procedure describes how to configure NSP to allow xDR export from ProTrace application to customer's external FTP or SFTP server.

1. **Copy the FTP security file from the NSP server**
   a) Open a terminal window and log in as root on the NSP server.
   b) As root, run:

   ```
   #  cd /opt/nsp/bea/user_projects/domains/tekelec/nsp
   ```

   c) Copy the contents of file sftp_security.pub.
2. **Update the FTP or SFTP server**
   a) Log in on the FTP or SFTP server.
   b) In the file $HOME/.ssh/authorized_keys, add the contents of file sftp_security.pub that you copied in the previous step.

c) Make sure that the FTP or SFTP server is properly configured to allow file transfer.

Change Customer Icon (*Optional*)

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

1. Open a terminal window and log in as `tekelec` on the NSP server.
2. Copy the customer icon file (`customer_icon.jpg`) to the `/opt/www/resources` directory.
3. Verify the customer icon properties:
   - The file name must be `customer_icon.jpg`.
   - The file must belong to user `tekelec` in group `tekelec`.
   - The compression format must be **Jpeg**.
   - Optimum width/height ratio is **1.25**.
   - Any image can be used; the suggested minimum width/height is **150** pixels.

Optional Post-Install Configuration Procedures

After NSP has been installed, there are optional configuration procedures that can be performed.

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 NSP server.

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

Configure Mail Server (*Optional*)

This procedure describes how to configure the SMTP mail server.

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

1. Open a terminal window and log in as `root` on the NSP server.
2. Enter the **platcfg** menu. As `root`, run:
   ```
   # su - platcfg
   ```

3. Select **NSP Configuration ➤ SMTP Configuration**.
4. Select **Edit**.
5. Type the IP address of the SMTP server and click **OK**.
   The host file for the alias used in the WebLogic Mail service is updated.
6. Exit the **platcfg** menu.

Configure Authenticated Mail Server (*Optional*)

This procedure describes how to authenticate the mail server. This procedure is optional.

Note: This procedure is performed ***after*** the SMTP has been configured (refer to the *#unique_72* procedure).

When a mail server requires authentication, additional parameters must be defined in the WebLogic console.

1. Connect to the NSP application interface.
2. Log in as `weblogic` on the WebLogic Console.
3. Select **Services ➤ Mail Sessions ➤ NspMailSession**.
4. Click **Lock&Edit** and modify the JavaMail properties as needed.

   For example:

   ```
   mail.transport.protocol=smtp,
   mail.smtp.host=mail.server,
   mail.smtp.from= noreply@tekelec.com,
   mail.smtp.timeout=500,
   mail.smtp.connectiontimeout=500
   ```

5. Add the following parameters:

   ```
   mail.smtp.auth=true
   mail.smtp.port=465
   mail.smtp.quitwait=false
   user=my_account
   password=my_password
   ```

   where *my_account* and *my_password* change according to the customer SMTP server.

6. If the SMTP over SSL is used, then add the following parameters:

   ```
   mail.smtp.socketFactory.port=465
   mail.smtp.socketFactory.class=javax.net.ssl.SSLSocketFactory
   mail.smtp.socketFactory.fallback=false
   ```

7. Click **Save**.
8. Click **Activate Configuration**.
9. Log in as `root` on the NSP server and run:

   ```
   # service nspservice restart
   ```

Configure SNMP Management Server (*Optional*)

This procedure describes how to configure the SNMP management server.

This procedure is optional; however, this option is required for Forwarding (forwarding by SNMP filter defined) and is available only on the NSP server.

1. Open a terminal window and log in as `root` on the NSP server.
2. Copy the files `server.crt` and `server.key` that are provided by the customer to `/root`.
3. Enter the **platcfg** menu. As `root`, run:

   ```
   # su - platcfg
   ```

4. Select **NSP Configuration ➤ SNMP Agent Configuration**.
   A window appears which allows you to enter the IP address of the SNMP management platform and version of SNMP agent and traps.
5. Select **Edit**.
6. Type the appropriate values and click **OK**.
   The SNMP agent configuration is updated and the SNMP Management server is automatically restarted.
7. Exit the **platcfg** menu.

Modify WebLogic Administration Password (*Optional*)

This procedure describes how to modify the WebLogic administration password.

This procedure is optional; however, this option is required for security and is available only on the NSP server.

1. Open a terminal window and log in as `root` on the NSP server.
2. Enter the **platcfg** menu. As `root`, run:

   ```
   # su - platcfg
   ```

3. Select **NSP Configuration ➤ NSP Password C onfiguration ➤ Weblogic Password Configuration (for startup and deploy)**.
   A window appears which allows you to enter the password. The password must contain at least 1 non-alphabetical character.
4. Select **Edit**.
5. Type a valid password and click **OK**.

   Note: Make sure the new password contains at least one numeric or special character.

   The configuration files are updated and NSP is restarted automatically.
6. Exit the **platcfg** menu.

Configure Session Timeout (*Optional*)

This procedure describes how to configure the session timeout, the amount of time (in minutes) that a session can remain inactive before it is invalidated and token released.

1. Log in as `TklcSrv` on the NSP application interface.
2. Select the **Security** application.
3. Select **Action ➤ Manage Tokens**.
   The **Tokens** window appears.
4. Type the appropriate value (in minutes; must be from 15 to 480, e.g., `30`) in the **Session timeout** field and click **Apply**.

Control Access of NSP to HTTPS (*Optional*)

This procedure describes how to control the access (enable or disable) of the NSP front-end to HTTPS. This procedure is optional.

1. Open a terminal window and log in as `root` on the NSP server.
2. Enter the **platcfg** menu. As `root`, run:

   ```
   # su - platcfg
   ```

3. Select **NSP Configuration ➤ Enable HTTP Port ➤ Edit**.
4. Select the appropriate option to either enable or disable the access and click **OK**.
   - Select **Yes** to enable access to HTTP.
   - Select **No** to disable access to HTTP.
5. Exit the **platcfg** menu.

Configure External LDAP (*Optional*)

This procedure describes how to use a customer-provided authentication based on the Lightweight Directory Access Protocol (LDAP). This procedure is optional.

1. Open a terminal window and log in as `root` on the NSP server.
2. Configure the NSP database. As `root`, run:

   ```
   # cd /opt/nsp/scripts/procs
   # sh nsp_update_procs.sh externalLDAP true
   ```

3. From a web browser, connect to the NSP application interface. Use the following URL:

   ```
   http://192.168.1.1/console
   ```

   where `192.168.1.1` is the IP address of the NSP server.
4. Log in to the WebLogic Console as `weblogic`.
5. Select **Security Realm ➤ myrealm ➤ Providers ➤ Authentication**.
6. Click **Lock&Edit** and add a new LDAPAuthenticator.

   Provide the necessary parameters that correspond to the customer LDAP tree configuration (refer to the *WebLogic* documentation for more information about this process).
7. Set the control flag for all of the Authentication Providers to **SUFFICIENT**.
8. Click **Save**.
9. Click **Activate Configuration**.

Chapter 4

Customer Integration Procedure

Topics:

This section provides the procedure to be performed at customer site. This procedure covers IP address change on external network.

Update External DIH IP Addresses

This procedure describes how to update external IP addresses and default route on DIH setup for TVOE, NSP, Oracle and IXP components.

1. External IP change procedure for TVOE and Oracle components

   Note: Repeat this step for TVOE host if needed and Oracle guests.

   a) Open a terminal window and log in to the host/guest as `root`.
   b) Enter the platcfg menu. As `root` run:

   ```
   # su - platcfg
   ```

   c) Navigate to **Network Configuration** ➤ **Network Interfaces** ➤ **Edit Interface**.
   d) Select an interface with external IP assigned.
   e) Click on **Edit**.
   f) Enter new external IP address and click **OK**. Wait until system reconfigures and navigate back to platcfg root menu.
   g) Navigate to **Network Configuration** ➤ **Routing** ➤ **Edit Default Route**. Edit the default route and click **OK**.
   h) Leave platcfg menu.

2. External IP change procedure for IXP component

   a) Open a terminal window and log in to IXP guest as `root`.
   b) Update `/root/bulkconfig` file with new external IP addresses. Change default gateway if needed.
   c) As `root` run:

   ```
   # bc_adjust_subsystem.sh
   ```

   Wait until system reconfigures.

3. External IP change procedure for NSP component

   a) Follow step 1 for changing system IP.
   b) Enter the platcfg menu. As `root` run:

   ```
   # su - platcfg
   ```

   c) Navigate to **NSP Configuration** ➤ **IP Configuration**and select **Edit** Button. Enter "Yes" on the confirmation dialog if the step "a" was executed successfully to change the IP.

Chapter

5

Incremental Upgrade Procedures

Topics:

This section provides the procedures for incremental upgrade of the DIH applications running on the TVOE guest.

Upgrade NSP Guest

This section provides the procedures for upgrading the NSP application on the NSP guest.

NSP Pre-Upgrade Sanity Check

This procedure describes different steps to be followed for the Pre-Upgrade Sanity tests.

1. **Remove the files to create space in /var/TKLC partition**

   a) Remove the old ISO.

   As `root` run:

   ```
   # rm –rf /var/TKLC/upgrade/*.iso
   ```

   Note: After removing these files, check minimum free disk space in /var/TKLC partition by the command 'df -h /var/TKLC'. If total available space is still less than 2.0 GB approx then procedure might fail.

2. **PreUpgarde Verification**

   a) Copy the NSP ISO to NSP Server (at /var/TKLC/upgrade) or Primary Weblogic server (In case of Fourbox configuration)

   b) Login as a Root user and execute the following command to mount the NSP iso
   As a root run :

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

   Where iso_path is the path of iso-image

   c) Run healthcheck:

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

   d) The logs are available at `/var/log/nsp/install/nsp_install.log`

   e) Check the message on terminal console.

   State and **Health** should be **RUNNING** and **OK** for all three servers.

   f) Verify that the build version should display the current release number. For example , if release is 7.1 then “7.1.0-X.Y.Z should be the new build number" and for 8.0 release "8.0.0-X.Y.Z should be the current build number" .

   g) Verify the RAM Size is [OK]

   Verify the space in /opt ,/tmp, /var/TKLC is [OK]

   If the space is [NOT OK] in any of the above partition,execute the following command to create some default space.

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

   type `yes` to continue
   Again run

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

   to verify the space is [OK]

If the space is [NOT OK] in any of the above partition contact Tekelec Technical services and ask for assistance.

h) Verify the free space in / , /opt/oracle is [OK].

If the space is [NOT OK] in any of the above partition contact Tekelec Technical services and ask for assistance.

i) Verify /tekelec SYMLINK is present [OK].

If /tekelec SYMLINK is not present contact Tekelec Technical services and ask for assistance.

3. **Pause JMS Consumption and Purge Terminated Alarms**

a) Execute the following command

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

b) Type `yes` to continue for purging of terminated alarms.
To purge terminated Alarms `enter 1` or to purge All Alarms `enter 2`

c) Execute the following command to unmount the NSP iso

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

d) Execute the following command to remove the NSP iso: `# remove /var/TKLC/upgrade/*.iso`.

4. **Remove Backout Files**

- **Note:** You need to login as a root user on Application Server.

a) Run the command to check if backout file exist.

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

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

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

NSP Pre-upgrade Settings

This procedure describes different steps to follow before running incremental upgrade.

1. **Login**
Login as root user on NSP Server.

2. **Check minimum free disk space in /var/TKLC partition**

a) As `root` run:

```
# df -kh /var/TKLC/
```

Example output:

```
Filesystem                        Size   Used   Avail   Use%   Mounted on
/dev/mapper/vgroot-plat_var_tklc  4.0G   1G     2.7G    47%    /var/TKLC
```

b) Check the space available under Avail column of this table. This should be at least 2.0 GB approx e.g.

in above table shown total space available is 2.7GB .

Note: If total available space is less than 2 GB, then do not continue with upgrade. Contact Tekelec Technical services and ask for assistance.

3. **Check minimum free disk space in /usr/TKLC/oracle/backup**

   Note: This step needs to be followed on Application Guest.

   a) As `root` run:

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

   Example output:

   ```

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

   b) Check the space available under Avail column of this table. This should be at least 15-20 GB approx e.g.

   in above table shown total space available is 57GB .

   Note: This step needs to be followed on Application Guest

4. **Verify Backup**

   a) On a daily basis, verify that the following files are backed up into a timestamped directory (NSP_BACKUP_TIMESTAMP) in the /opt/oracle/backup/ directory in NSP Guest.

   For Example :

   ```
   # drwxrwxrwx 2 root root 4096 Dec 21 22:00 NSP_BACKUP_07_13_09_22_00_00
   ```

   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.

   Note: If **Application_BACKUP_TIMESTAMP** directory is not available then follow the commands mentioned below to generate the Application_BACKUP_10_08_11_22_00_01:

   Login to NSP Guest as a `root` user.

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

   ```
   #  ./LaunchExpNSPdp.sh
   ```

   The nightly backup will be generated inside `/opt/oracle/backup` directory.

5. **Set the Changed password for tekelec user**

   Note: This step is only applicable for Onebox configuration.

   Note: This configuration is required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined and no server address override defined by app)

   a) Enter platcfg configuration menu.

b) From main platcfg menu, navigate to **NSPConfiguration ➤ NSP Password Configuration ➤ NSP Password Configuration (for update/upgrade)**
c) Enter the current password for tekelec user of NSP GUI in the text box and select OK.

Note:

1. Please verify it is the correct password otherwise upgrade may fail.
2. Password entered during this procedure will not be displayed in platcfg until the upgrade procedure is completed.

Backup NSP Database

This section describes the various steps for taking the backup of NSP database.

Take the NSP Backup

a) Login as `root` on NSP Guest

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

```
#  ./LaunchExpNSP.sh /opt/oracle/backup/upgrade_backup
```

The backup will be generated on NSP Guest inside `/opt/oracle/backup/upgrade_backup/` directory. If there is any previous backup available inside`/opt/oracle/backup/upgrade_backup/` , please remove that backup directory.

NSP Incremental Upgrade

This procedure describes different steps to follow for running incremental upgrade.

1. **Distribute the NSP ISO**
   a) Distribute the NSP ISO file to `/var/TKLC/upgrade` directory or insert the NSP DVD.
      - On the rackmount server copy the NSP ISO into the `/var/TKLC/upgrade` using the scp command.
      - 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 NSP ISO is not present in the PM&C ISO repository, add the ISO file.

   b) Then open a terminal and login as root user to the server you are about to install.
2. **Initiate upgrade**
   a) To enter platcfg menu, as root run:

   ```
   # su - platcfg
   ```

   b) From the main platcfg menu, navigate to **Maintenance ➤ Upgrade** and select **Initiate Upgrade.**
   c) Wait until installation is finished.

   Server will be restarted automatically if installation ends without errors.

   d) Check the NSP installation log `/var/TKLC/log/upgrade/upgrade.log` for any errors.
3. **Remove NSP iso from /var/TKLC/ upgrade**

Note: This steps is applicable only if the upgrade was done using ISO.

a) Remove NSP iso from `/var/TKLC/upgrade` after successful incremental upgrade.

Upgrade A-Node

Upgrade Node A

Follow the procedure below only if there is a change in XMF ISO .

Configure Node A and Restart NTP

NSP Post-Upgrade Check

This procedure describes different steps to be followed for the Post-Upgrade Sanity tests.

1. **WebLogic Console**

   a) From Internet Explorer, connect to the WebLogic console using the following URL:

   http://192.168.1.1/console

   Where **192.168.1.1** is the IP address of the NSP Server.

2. **Login**

   a) You should be prompted to "Log in to work with the WebLogic Server domain ".

   Connect with User **weblogic**

3. **Console Display**

   a) Under the **Environment** heading, click on the **Servers** link.

4. **Health Check**

   a) On clicking the "Servers" link in the last step, the console would display the **Summary of Servers**, with a list of the three servers, nsp1a, nsp1b and nspadmin.

   b) Entries in the columns **State** and **Health** should be **RUNNING** and **OK** for all three servers.

5. **Resume JMS Consumption**

   a) Open a terminal console using root user on NSP server

   b) Execute the command below to resume JMS consumption

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

6. **NSP GUI**

   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 NSP Server.

   b) If it is a Fourbox Configuration, enter the IP of the Apache server.

7. **Login**

   a) Login to the Application with User name **tekelec**

8. **Portal**

   a) In the top frame, on mouse-over on the link **Portal**, click on the **About** link that will be displayed.

b) A pop-up window with the build information will be displayed.

9. **Build Verification**

   a) The build version should display the current release number. For example , if release is 7.1 then “7.1.0-X.Y.Z should be the new build number" and for 8.0 release "8.0.0-X.Y.Z should be the new build number" .

10. **Check Oracle Enterprise manger connection**

    a) From Internet Explorer, connect to the following URL: *https://192.168.1.1:1158/em*

    Where **192.168.1.1** is the IP address of the Oracle server.

    b) You should be prompted to log in to work with the Enterprise manager.

    Connect with User **nsp.**

Upgrade PMF Guest

This section provides the procedures for upgrading the PMF application on the PMF guest.

xMF Pre-Upgrade 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. **Run the automatic healthcheck script and verify output**

   a) Run analyze_subsystem.sh script:

   ```
   $ analyze_subsystem.sh
   ```

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

   If the error occurs, contact the 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!
```

2. **Synchronize NSP with IMF**
    a) From supported browser login to the NSP Application GUI as privileged user.
    b) Go to the Centralized Configuration.
    c) Navigate to **Acquisition** in left tree panel.
    d) Navigate to the site.
    e) Right click on subsystem and click on **Synchronize** option on menu.
    f) This will synchronize the links.
    g) Right click on subsystem and click on **Apply Changes** option on menu.

Upgrade PMF Guest

If upgrading a provisioned system, notify potential users to not start the provision using the software during the duration of the upgrade.

Upgrade PMF from PM&C GUI

a) Open a web browser and log in to the PM&C application interface as pmacadmin.
b) Navigate to **VM Management**.
c) A **VM entities** list will appear. Click on particular TVOE host blade server (identified by *Enc:id Bay:id*).
d) A sublist with guests will appear. Click on a particular guest.
e) Click on **Upgrade**. A list of available ISOs will appear.
f) Select the new PMF application ISO and click on **Start Upgrade**. An application upgrade will be triggered.
g) Observer **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Check status that the application has been upgraded successfully.

Sync NSP with xMF

1. **Synchronize xMF Applications**

   a) From supported browser login to the NSP Application GUI as privileged user
   b) Go to the Centralized Configuration
   c) Navigate to **Acquisition 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**)

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!
```

Upgrade IXP Guest

This section provides the procedures for upgrading the IXP application on the IXP guest.

IXP Subsystem Healthcheck

This procedure describes how to run the automatic healthcheck of the IXP guest. This healthcheck also checks the Oracle guest has started as in operational state.

1. Open a terminal window and log in on any IXP server in the IXP subsystem you want to analyze.
2. As `cfguser`, run:

   ```
   $ analyze_subsystem.sh
   ```

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

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

   Example of overall output:

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

```
END OF ANALYSIS OF SERVER ixp2222-1b

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

Example of a successful test:

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

Example of a failed test:

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

3. Run Oracle guest healthcheck.
   a) Open a terminal window and log in to Oracle guest as `grid` user.
   b) As `grid` run:

      ```
      $ crsctl status resource -t
      ```

   c) Once the Oracle stack has fully started, the output should be as follows where the STATE_DETAILS of the database resource (ora.pic.db) equals "Open".

      ```
      ---------------------------------------Open-----------------------------
      NAME          TARGET  STATE        SERVER                   STATE_DETAILS
      -----------------------------------------------------------------------------
      Local Resources
      -----------------------------------------------------------------------------
      ora.DATA.dg
                    ONLINE  ONLINE      ora
      ora.LISTENERASM.lsnr
                    ONLINE  ONLINE      ora
      ora.asm
                    ONLINE  ONLINE      ora                      Started
      ora.ons
                    ONLINE  ONLINE      ora
      -----------------------------------------------------------------------------
      Cluster Resources
      -----------------------------------------------------------------------------
      ora.cssd
            1        ONLINE  ONLINE      ora
      ora.diskmon
            1        ONLINE  ONLINE      ora
      ora.evmd
            1        ONLINE  ONLINE      ora
      ora.pic.db
            1        ONLINE  ONLINE      ora                      Open
      ```

IXP Incremental Upgrade Procedure

If upgrading a provisioned system, notify potential users to not start the provision using the software during the duration of the upgrade.

1. Open a web browser and log in to the PM&C application interface as pmacadmin

2. Navigate to **VM Management**.
3. A **VM entities** list will appear. Click on particular TVOE host blade server (identified by `Enc:id Bay:id`).
4. A sublist with guests will appear. Click on a particular guest.
5. Click on **Upgrade**. A list of available ISOs will appear.
6. Select the new IXP application ISO and click on **Start Upgrade**. An application upgrade will be triggered.
7. Observe **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Check the status to confirm that the application has been upgraded successfully.
8. Login to the IXP guest as root and run the following command to finish the upgrade:

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

Discover IXP application in CCM

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

1. **Discover all IXP servers in Centralized Configuration application.**
   a) Open a web browser and go to the NSP application interface main page.
   b) Click **Centralized Configuration**.
   c) Navigate to **Equipment reqistry** view.
   d) Open **Sites**, open the site, open **IXP** and then click on the particular IXP subsystem.
   e) The list of all IXP servers in the IXP subsystem will appear. Check the check box of the first server and click the **Discover Applications** button. Wait until the IXP application will be discovered. Then repeat this step for all servers in the subsystem.
2. **Apply the configuration to the IXP subsystem**
   a) Go back to NSP GUI main page.
   b) Click **Centralized Configuration**.
   c) Navigate to the **IXP** view.
   d) Open **Sites**, open the site, open **IXP**.
   e) Right-click on the subsystem and click on **Apply Changes**.
   f) Click **Next** button.
   g) Click **Apply Changes** button.
   h) Wait until changes are applied.

   Check there's no error in the result window.

Configure JmxAgent

This procedure describes how to configure the JmxAgent to allow HTTP access.

1. Open a terminal window and log in as `cfguser` on the IXP server.
2. Edit `/opt/TKLCjmxagent/in/agent.properties`
3. Change `HttpAdaptor=false` to `HttpAdaptor=true`
4. Save changes
5. Restart JmxAgent by command:

```
# pm.kill JmxAgent
```

Centralized xDR Builders Upgrade

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

1. **Install Builder ISO on NSP**
   a) Copy the xDR builder ISO to the NSP server or insert the xDR Builder CD.
   b) Open a terminal window and log in on the NSP server as root.
   As root run:

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

   c) Confirm this operation if you will be prompted to do so. You will be asked to enter path to the media:

   ```
   Please enter path to Builder CDROM or ISO [/media/cdrom]
   ```

   Choose one of the following options:

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

   d) Wait until installation finishes.
2. **Verify the ISO installation on NSP.**
   a) Open a web browser and login to the NSP application interface as the `TklcSrv` user.
   b) Click **Upgrade Utility**
   c) Click on **Manage Builder Rpm** on the left tree.

   It will display the list of the xDR builder rpms. One of them is the one that belongs to the ISO file installed in the previous step. The state will be **Not Uploaded**.
3. **Dry run**
   a) Click on **Manage Builder Rpm** on the left tree.

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

   b) Dry Report will be generated for each dictionary indicating change to be done (`Added/Removed/Deprecated field(s)`).

   This report will also display configuration which are using deprecated field and configurations which will become incompatible after removal of field.

   Before Proceeding with Further steps read Notes below and plan accordingly for execution of builder upgrade.

   Note: Configurations (Query/Protraq/xDR Filter) on the removed Field must be modified prior to builder upgrade so as to remove the used of removed field. Otherwise the configurations will become incompatible after uploading the builder RPM from NSP.

   Note: Configurations (Query/Protraq/xDR Filter) on the deprecated Field can continue to work after builder upgrade. Use of deprecated field is supported till two releases after that the field will be marked for Removal.

Note: XDR builder Upgrade will not upgrade the static enrichment, they should be upgraded manually.

Note: If the configurations on removed field are large, please prepare for this in advance as it can consume significant amount of time

4. **Upload Builder RPM**
   a) Mark the requested builder RPM with the **Not Uploaded** state and press **Upload** in the toolbar.
   b) A dialog box will appear.

      Click on **Continue** to continue the RPM upload.
   c) After the successful upload the RPM state will change to **Uploaded**
5. **Associate xDR builders RPM with the IXP subsystem**
   a) Click on **View Builder RPM Status** link on the left tree.

      This will display a list of all IXP subsystems.
   b) Choose one IXP subsystem and click on **Associate RPM Package** icon in the tool bar.

      This will show a popup containing the list of builder RPMs that are uploaded in NSP.
   c) Select required xDR builders RPM and click on the **Associate** button.
   d) After the successful association the list of the subsystems will be updated.

      The **RPM Name** column will contain the new RPM package name and **Association Status** will be marked as OK.
6. **Apply the configuration to the IXP subsystem**
   a) Go back to NSP GUI main page.
   b) Click **Centralized Configuration**.
   c) Navigate to the **IXP** view.
   d) Open **Sites**, open the site, open **IXP**.
   e) Right-click on the subsystem and click on **Apply changes…** from popup menu.
   f) Click **Next** button
   g) Click **Apply Changes** button.
   h) Wait until changes are applied.

      Check there’s no error in the result window.
7. **Install Builder RPM on IXP**
   a) Go back to NSP GUI main page.
   b) Click **Upgrade Utility**.
   c) Click on **View Builder RPM Status** from the left tree.

      This will display all the available IXP subsystem with their respective RPM **Associate Status** and **Install Status**.
   d) Before initiating the builder installation make sure the **Builder RPM** that you want to install on the IXP subsystem is associated with the IXP subsystem as indicated by **RPM Name** column and **Association Status** should be OK and **Install Status** should be either **-** or **Not Started**.
   e) Select one or more IXP subsystem and choose **Install RPM Package** from the tool bar.
   f) After the successful installation the **Install status** will change to OK.

Oracle Incremental Upgrade Procedure

Oracle TPD is used to upgrade the TPD installation and associated rpms, the oracle instance is not upgradeable, as such you must use the oracle-tpd ISO to perform all upgrades of DIH Oracle. Note: Be sure to use oracle-tpd ISO for upgrades.

1. Prior to upgrade run the Oracle health check.
    1. As grid run: `$ crsctl status resource -t`
    2. Once the Oracle stack has fully started, the output should be as follows where the STATE_DETAILS of the database resource (ora.pic.db) equals "Open".

```
---------------------------------------Open-----------------------------
NAME TARGET STATE SERVER STATE_DETAILS
-----------------------------------------------------------------------------
Local Resources
-----------------------------------------------------------------------------
ora.DATA.dg
ONLINE ONLINE ora
ora.LISTENERASM.lsnr
ONLINE ONLINE ora
ora.asm
ONLINE ONLINE ora Started
ora.ons
ONLINE ONLINE ora
-----------------------------------------------------------------------------
Cluster Resources
-----------------------------------------------------------------------------
ora.cssd
1 ONLINE ONLINE ora
ora.diskmon
1 ONLINE ONLINE ora
ora.evmd
1 ONLINE ONLINE ora
ora.pic.db
1 ONLINE ONLINE ora Open
```

2. Shutdown the ixp and nsp guests before Oracle upgrade. Log in to the TVOE host as root.
    1. As root on the tvoe host run the virsh console command and log in to the nsp guest.

       `[root@tvo ~]# virsh console nsp`
    2. As root on the nsp shutdown the nsp guest.

       `[root@nsp ~]# init 0`
    3. As root on the tvoe host run the virsh console command and log in to the ixp guest.

       `[root@tvo ~]# virsh console ixp`
    4. As root on the ixp shutdown the ixp guest.

       `[root@ixp ~]# init 0`

3. Upgrade Oracle from PM&C GUI

   Note: The following steps describes how to Upgrade Oracle guest using PM&C.

1. Open a web broswer and log in to the PM&C interface as `pmacadmin`
2. Navigate to VM Management.
3. A VM entities list will appear. Click on particular TVOE host blade server (identified by `Enc:id Bay:id`).
4. A sublist with guests will appear. Click on the Oracle guest.
5. Click on Upgrade. A list of available ISOs will appear.
6. Select the Oracle-Tpd ISO and click on Start Upgrade. An Oracle TPD upgrade will be triggered.
7. Observe Task Monitoring page for upgrade progress. Wait until the upgrade is finished.

4. Startup the IXP and NSP guests on the TVOE host.

   ```
   [root@tvo ~]# virsh start nsp
   ```

   Domain nsp started

   ```
   [root@tvo ~]# virsh start ixp
   ```

   Domain ixp started

5. After the upgrade run the Oracle healthcheck.

   1. As grid run:

      ```
      $ crsctl status resource -t
      ```

   2. Once the Oracle stack has fully started, the output should be as follows where the STATE_DETAILS of the database resource (ora.pic.db) equals "Open".

      ```
      ---------------------------------------Open-----------------------------
      NAME TARGET STATE SERVER STATE_DETAILS
      -----------------------------------------------------------------------------
      Local Resources
      -----------------------------------------------------------------------------
      ora.DATA.dg
      ONLINE ONLINE ora
      ora.LISTENERASM.lsnr
      ONLINE ONLINE ora
      ora.asm
      ONLINE ONLINE ora Started
      ora.ons
      ONLINE ONLINE ora
      -----------------------------------------------------------------------------
      Cluster Resources
      -----------------------------------------------------------------------------
      ora.cssd
      1 ONLINE ONLINE ora
      ora.diskmon
      1 ONLINE ONLINE ora
      ora.evmd
      1 ONLINE ONLINE ora
      ora.pic.db
      1 ONLINE ONLINE ora Open
      ```

TVOE Upgrade Procedure

TVOE guest must be shutdown before TVOE upgrade is performed per 909-2211-001 2.3 TVOE 2.x Softwre Upgrade Procedure Upgrade Flow "Application Guest Shutdown Procedure." TVOE upgrade accpet/reject that will also require the guests to be shutdown gracefully again just prior to accept.

Note: Upgrade to TVOE should not be performed unless directed to do so.

TVOE upgrade accept/reject that will also require the guests to be shutdown gracefully again just prior to the accept.

```
virsh console nsp

[root@nsp ~]# init 0

virsh console ixp

[root@ixp ~]# init 0

virsh console ora

[root@ora ~]# init 0

virsh console pmf

[root@pmf ~]# init 0
```

Chapter 6

DIH Disaster Recovery Procedure

Topics:

This section provides the procedures for DIH Disaster Recovery. DIH Disaster recovery procedure does not preserve the data that are stored in the Oracle database. Only DIH system configuration data are preserved. Fresh install of TVOE and associated application guests are part of the disaster recovery procedure.

Disaster Recovery is the methodology used to recover from a failed upgrade procedure (Major: 1.x to 2.x or Minor: 1.1.x to 1.2.x) as well as recovery from a catastrophic failure.

1. Backup configuration data. Refer to *DIH Configuration Backup*
2. Destroy application guests and sidecar partitions. Refer to *Clean Up TVOE Guests and Sidecar Partitions*
3. Perform fresh install procedure. Refer to flowchart *DIH Installation Overview*
4. Restore configuration data. Refer to *DIH Configuration Restore*

DIH Configuration Backup

This section provides the procedure to backup the DIH configuration.

NSP Backup Procedure

Steps for NSP Backup

a) Open a terminal window and log in to NSP Guest as `root`.

b) Execute the following commands

As `root` run:

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

```
#  ll
```

Output will be something like:

```
[root@nsp backup]# ll
total 36
drwxrwxrwx 5 root root  4096 Oct  7 22:00 NSP_BACKUP_10_07_11_22_00_01
drwxrwxrwx 5 root root  4096 Oct  8 22:00 NSP_BACKUP_10_08_11_22_00_01
```

c) Copy the **NSP_BACKUP_10_08_11_22_00_01** directory with latest timestamp to an external device.

Note: Please make sure the Backup which is getting copied is of same Application release , which is currently installed.

Note: If **Application_BACKUP_TIMESTAMP** directory is not available then follow the commands mentioned below to generate the Application_BACKUP_10_08_11_22_00_01:

Login to NSP Guest as a `root` user.

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

```
#  ./LaunchExpNSPdp.sh
```

The nightly backup will be generated on NSP Guest inside `/opt/oracle/backup` directory. Copy the **NSP_BACKUP_10_08_11_22_00_01** directory to an external device.

Clean Up TVOE Guests and Sidecar Partitions

This procedure describes how to destroy application guests that are configured on TVOE. Also this procedure will clear a sidecar partitions.

1. **Destroy all TVOE guests**

a) Open a terminal window and log in to TVOE host as `root`.

b) List all available guests that are created on the TVOE host.

As `root` run:

```
# virsh list
```

Example:

```
[root@opica ~]# virsh list
Id Name State
----------------------------------
17 ixp running
26 ora running
38 nsp running
42 pmf running
```

c) Destroy all guests. For each guest as `root` run:

```
# virsh destroy guest_name
```

where *guest_name* is the name of the guest from previous step.

2. **Clean Sidecar Partitions**

a) As `root` run:

```
# lvremove -f /dev/external/*
# vgremove external
# pvremove /dev/cciss/c0d0
# hpacucli ctrl slot=3 ld all delete forced
```

DIH Configuration Restore

This section provides the procedure to restore the DIH configuration.

Import NSP Database and Restore Realm backup

This section describes the various steps and methods for importing NSP database.

1. **Stop WebLogic**

a) Login as `root` user on NSP Guest.

As `root` run:

```
# service nspservice stop
```

2. **Import NSP backup**

a) Login as `root` user on Oracle Guest.

b) Copy the oracle-scripts.tar which is present on NSP Guest, into `/tmp` of Oracle Guest.

```
# scp nsp_ip:/opt/nsp/scripts/oracle-scripts.tar /tmp
```

where *nsp_ip* is the IP address of NSP Guest

c) Copy the **NSP_BACKUP_10_08_11_22_00_01** directory on Oracle Guest and change the permission using following command.

```
# chmod -R 777 <<backup_dir>>
```

where *backup_dir* will be the path to NSP_BACKUP_10_08_11_22_00_01 directory.

d) Execute the following commands.

```
# cd /tmp/
```

```
# tar xf oracle-scripts.tar
```

```
# chmod -R 777 /tmp/oracle/
```

```
# su - oracle
```

```
# cd /tmp/oracle/cmd/
```

```
# ./GenScripts.sh NSP/NSP NSP
```

```
# ./LaunchNSPTruncate_1.sh
```

```
# ./ImpNSPdp.sh NSP/NSP NSP NSP <<backup_dir>>
```

The ImpNSPdp.sh script has four parameters.

- Oracle connection string (NSP/NSP) must not be modified
- Name of the exported schema name (NSP) must not be modified
- Target schema name (NSP) must not be modified
- The *backup_dir* is the path of the directory which contains the exported database file(ExpNSP.dmp.gz).(e.g. `/opt/oracle/backup/NSP_BACKUP_10_14_10_22_00_01/oracle/`)

```
# ./LaunchNSPTruncate_2.sh
```

3. **Restore Realm backup**

a) Login as `root` user on DIH NSP setup.
b) Copy the realm backup into a local directory.
c) Execute the following commands.

Note: Make sure the backup is from the same Application release which needs to be imported

As `root` run:

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

where *backup_dir* is the directory which contains the backup of realm data (e.g. `/opt/oracle/backup/NSP_BACKUP_10_14_10_22_00_01/`)

4. **Restart weblogic**

a) As a `root` user on NSP Guest , execute the following command.

```
# service nspservice start
```

Restore Configuration on IXP and PMF

This section describes the various steps and methods for importing NSP database.

1. **Clean current PMF configuration**

a) Open a terminal window and log in to the PMF guest as `cfguser`.
b) Clobber the IDB. As `cfguser` run:

```
$ prod.start -C
```

c) Delete `/opt/TKLCjmxagent/in/ccm-config.properties` file.

2. **Open a web browser and log in to the NSP application interface to apply changes to PMF guest to restore the configuration.**
   a) To Apply Changes for each subsystem go to **Acquisition ➤ Sites ➤ XMF.**
   b) Right click on subsystem and click on **Apply Changes** option on menu.

   Note: If 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. **Clean current IXP configuration**
   a) Open a terminal window and log in to the IXP guest as `cfguser`.
   b) Clobber the IDB. As `cfguser` run:

   ```
   $ prod.start -C
   ```

   c) Delete `/opt/TKLCjmxagent/in/ccm-config.properties` file.
4. **Open a web browser and log in to the NSP application interface to apply changes to IXP guest to restore the configuration.**
   a) Navigate to **IXP ➤ Sites** .
   b) Open **IXP**.
   c) Right-click the subsystem and select **Apply changes…**.
   d) Click **Next**.
   e) Click **Apply Changes**.
   f) Verify that there are no errors on the result page that will display. If there are any errors contact the Tekelec Customer Care Center.

Chapter 7

External Software Configuration

Topics:

This section provide the procedures for external software configuration.

Installation of External Datawarehouse for DataExport

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

- Orale 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`

This procedure is applicable to Oracle 11g.

1. **Customer: Grant roles**

   Note: This step must be provided by the customer. 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.

   a) 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;
   ```

2. **Grant DBA role**

   a) Log in to any mediation server of the mediation subsystem that can reach the External DataWarehouse and is supposed to be a DataFeed application host for this External DataWarehouse as `cfguser`. Thus you will ensure the DTO package compatibility.

   As `cfguser` run:

   ```
   $ cd_oracle_utils
   $ ./GrantDbaRole.sh sys/sys_pass@ip/sid user_name
   ```

   where *sys_pass* is password for sys user, *ip* is IP address of external datawarehouse, *sid* is SID of the instance provided by customer and *user_name* is the user name of database user that will perform the installation and has granted the permissions in the previous step.

3. **Create the schema**

   a) As `oracle` (xDR Storage server) or `cfguser` (any other mediation server) run:

   ```
   $ /opt/TKLCmediation/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).

4. **Post-installation check**

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

   a) 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
   ```

5. **Install package, procedures and tables**

   Note: 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).

6. **Install and enable Oracle nightly jobs**

   a) 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.

7. **Revoke DBA role**

   a) As `cfguser` run:

   ```
   $ cd_oracle_utils
   $ ./RevokeDbaRole.sh sys/sys_pass@ip/sid user_name
   ```

   where *sys_pass* is password for sys user, *ip* is IP address of external datawarehouse, *sid* is SID of the instance provided by customer and *user_name* is the user name of database user that performed the installation and has granted the permissions in the step 2.

8. **WA 208358**: Oracle 11g to Oracle 10g Data Feed

   a) Open a terminal window and log in to ora guest as `oracle` user.

   b) Log in to Oracle console. As `oracle` run:

   ```
   $ sqlplus / as sysdba
   ```

   c) Grant catalog permission to `DTO_EXE` role:

   Run:

   ```
   SQL> GRANT SELECT_CATALOG_ROLE TO DTO_EXE;
   SQL> exit;
   ```

Chapter 8

Incremental Backout Procedures

Topics:

This section provides the procedures for incremental backout of the DIH applications running on the TVOE guest.

Incremental releases are defined for DIH as: 1.1.0 to 1.x.x to 1.1.0 to 2.x.x.

Incremental upgrades and backout are within with release build versions.

NSP One-box Incremental Backout Procedure

This procedure describes different steps to follow for running backout and it can be executed if the incremental upgrade fails.

1. **NSP package ISO**
   a) Copy the ISO of installed version of NSP to **`/var/TKLC/upgrade`** using SCP, rsync, etc..
   b) Then open a terminal window and login as `root` user. Mount the ISO.

   As `root` 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`).

2. **Run backout script**
   a) Remove any old scripts from `/tmp/scripts` folder

   As `root` run:

   ```
   # rm –rf /tmp/scripts
   ```

   b) Copy the scripts folder to the `/tmp` directory.

   As `root` run:

   ```
   # cp -rf /mnt/upgrade/scripts /tmp
   ```

   c) As `root` run:

   ```
   # chmod –Rf +x /tmp/scripts
   # dos2unix /tmp/scripts/*.sh
   ```

   d) Run the backout script.

   As `root` run:

   ```
   # sh /tmp/scripts/inc_backout_6.0.sh
   ```

   e) When prompted

   ```
   This will backout the upgrade of NSP release Type yes to continue
   ```

   type `yes`

3. **End of Installation and Backout verification**
   a) At the end of installation a message like the following will be displayed

   ```
   +++ E N D  O F   N S P   P A C K A G E   B A C K O U T
   ```

   b) Check `/var/log/nsp/install/nsp_install.log` for any erroneous message towards the end of log file
   c) From Internet Explorer, connect to the NSP Application GUI using the following URL: *http://NSP_GUI_IP/nsp*
   d) Login to the Application with User name **tekelec**
   e) In the top frame, on mouse-over on the link **Portal**, click on the **About** link that will be displayed.
   f) A pop-up window with the build information will be displayed.

g) The build version should display “Portal 7.1.x-X.Y.Z Where 7.1.x-X.Y.Z should be the old build number.

4. **Umount ISO**

   a) As `root` run:

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

5. **Mount the old NSP package DVD/ISO of source release(The software release from which the NSP was upgraded)**

   a) Insert NSP software DVD or copy the ISO to `/var/TKLC/upgrade` using SCP, rsync, etc..

   b) Then open a terminal and login as `root` user

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

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

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

6. **Install old NSP RPM**

   a) As `root` run:

   ```
   # rpm –ivh /mnt/upgrade/CentOS/tklc-nsp-${version}-${build}-i686.rpm --noscripts
    --justdb
   ```

   Note: version and build should be replaced by the version and build of Application DVD.

   ```
   Example: rpm –ivh /mnt/upgrade/CentOS/tklc-Application-7.1.0-4.8.0-i686.rpm
   ```

7. **Unmount the NSP ISO**

   a) Umount the drive.

   As `root` run:

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

8. **Node A Backout**

   a) If xMF backout is required, then backout Node A also.

   Follow the steps mentioned below.

   b) Login as root user on the NSP Server.

   As `root` run:

   ```
   # cd /mnt/upgrade/CentOS/RPMS
   # service TKLCmf stop
   # rpm –Uvh --force TKLCmf*.rpm
   # su – cfguser –c “setCCMnode NSP_Server_IP”
   ```

xMF Incremental Backout Procedure

No matter the initial cause of the upgrade problem, once all necessary corrective steps have been taken to prepare for the backout/rollback, then the following procedure can be executed to perform a backout/rollback.

Backout/rollback only supports backing out/rolling back 1 release.

Execute this procedure if the XMF server has been upgraded or partially upgraded using any non-live procedure.

Backout of xMF

a) Login as root on the xMF server

b) Change to the backout directory:

```
# cd /var/TKLC/backout
```

c) Execute the backout/rollback using the backout_server script:

```
# ./backout_server
```

Many informational messages appear on the terminal screen during backout/rollback.

d) When backout/rollback is complete, manually reboot the server.
# **reboot**

e) After the reboot, the screen displays the login prompt.

f) Change to the cfguser id:

```
# su - cfguser
```

g) Execute following command to set on NTPDeamon process after backout procedure:

```
$ pm.set on NTPDeamon
```

h) Exit back to root user:

```
$ exit
```

IXP Incremental Backout Procedure

This procedure describes the incremental backout procedure of the IXP guest from the new release to the old release. This procedure is not applicable to major backout procedure.

1. **Stop TKLCixp service**

   a) Open a terminal window and log in as `root` on the server you want to backout.

   b) Stop `TKLCixp` service

   As `root` run:

   ```
   # service TKLCixp stop
   ```

2. **Unmount NFS shares**

   As `root` run:

   ```
   # umount -a -l -t nfs
   ```

3. **Start backout procedure**

   a) Trigger server backout.

   As `root` run:

   ```
   # /var/TKLC/backout/backout_server
   ```

Example output:

```
Verifying that backout is possible.

Current platform version:  4.2.3-70.86.0
Backing out to platform version:  4.2.2-70.74.0

compare_platform_versions (4.2.3-70.86.0, 4.2.2-70.74.0)
compare with major upgrade boundary (3.0.0-60.0.0, 4.2.2-70.74.0)
compare with no backout boundary (4.0.0-70.0.0, 4.2.2-70.74.0)
Backout Date:  05/16/2011 15:45:53 UTC
Continue backout?  [y/N]:
```

b) Type `[y]` to continue and press `[ENTER]`.
c) Wait until backout is finished. Then reboot the server.

4. **Re-discover application in CCM**
   a) Open a web browser and log in to the NSP application interface as `TklcSrv` user.
   b) Click **Centralized Configuration**.
   c) Navigate to **Equipment registry** view.
   d) Open **Sites**, open the site, open**IXP** and then click on the particular IXP subsystem.
   e) The list of all IXP servers in the IXP subsystem will appear. Check the check box of the backouted server and click the **Discover Applications** button. Wait until the IXP application will be discovered.

xDR Builder Backout

This procedure describes the incremental xDR builder backout procedure.

1. **Create `/tmp/builder_backout` file on IXP server**
   a) Log in to the ActMaster server of the IXP subsystem where you want to backout xDR builders package as `root` user.
   b) As `root` run:

```
# touch /tmp/builder_backout
```

   c) **WORKAROUND PR204590:** Login to NSP Primary WebLogic server or NSP One-Box server as `root` and run:

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

   Check that the TKLCxdrbuilders RPM you are about to backout is listed. If the TKLCxdrbuilders RPM to which the backout should be done was removed from NSP server due to backout or disaster recovery of NSP server, upload the TKLCxdrbuilders rpm to `/var/TKLC/jmxagent/upload`. Then continue with this procedure.

2. **Associate xDR builders RPM with the IXP subsystem**
   a) Open a web browser and login to the NSP application interface as the `TklcSrv` user.
   b) Click **Upgrade Utility**
   c) Click on **View Builder RPM Status** link on the left tree.

   This will display a list of all IXP subsystems.

   d) Choose one IXP subsystem and click on **Associate RPM Package** icon in the tool bar.

This will show a popup containing the list of builder RPMs that are uploaded in NSP.

e) Select required xDR builders RPM and click on the **Associate** button.
f) After the successful association the list of the subsystems will be updated.

The **RPM Name** column will contain the new RPM package name and **Association Status** will be marked as OK.

3. **Apply the configuration to the IXP subsystem**

a) Go back to NSP GUI main page.
b) Click **Centralized Configuration**.
c) Navigate to the **IXP** view.
d) Open **Sites**, open the site, open **IXP**.
e) Right-click on the subsystem and click on **Apply changes…** from popup menu.
f) Click **Next** button
g) Click **Apply Changes** button.
h) Wait until changes are applied.

Check there's no error in the popup window.

4. **Install Builder RPM on IXP**

a) Go back to NSP GUI main page.
b) Click **Upgrade Utility**.
c) Click on **View Builder RPM Status** from the left tree.

This will display all the available IXP subsystem with their respective RPM **Associate Status** and **Install Status**.

d) Before initiating the builder installation make sure the **Builder RPM** that you want to install on the IXP subsystem is associated with the IXP subsystem as indicated by **RPM Name** column and **Association Status** should be OK and **Install Status** should be either **-** or **Not Started**.
e) Select one or more IXP subsystem and choose **Install RPM Package** from the tool bar.
f) After the successful installation the **Install status** will change to OK.

5. **Session Upgrade**

a) Go back to NSP application interface main page.
b) Click **Upgrade Utility**.
c) Click **Upgrade Session** link on left tree, this display all the sessions to be upgraded due to upgrade of associated dictionary.
d) Select one or more session(s) (use ctrl key for selecting multiple sessions) with **Session Upgrade Status** as either **Need Upgrade** or **Error** and choose **Upgrade** icon from tool bar.

You may use available quick filter options on this list page to filter out sessions which you want to upgrade in one go.

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

Once upgrade is initiated for a session, its **Upgrade Status** will become **Upgrade Intiated**.

e) Once session is upgraded its **Upgrade Status** will become **Upgraded Successfully**.

6. **Remove `/tmp/builder_backout` file on IXP server**

a) Log in to the ActMaster server of the IXP subsystem where you created `/tmp/builder_backout` file as `root` user.

b) As `root` run:

```
# rm /tmp/builder_backout
```

Appendix A

DIH Bulkconfig File Description

Topics:

This section provides the bulkconfig file descriptions for DIH application components.

DIH Common Bulkconfig File Description

The DIH common `bulkconfig` file contains the overall DIH pre-installation configuration information (except PMF). During the installation process, various scripts use this file to configure the DIH.

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 DIH bulkconfig file template is located on the IXP iso on the `/upgrade/DIH_bulkconfig_template` path.

Note: When you install DIH, you are asked to create this `bulkconfig` file and update this file. **DO NOT** remove the DIH `bulkconfig` file from the server.

The DIH `bulkconfig` contains the following configuration information:

- TVOE host configuration
- NSP guest configuration
- IXP guest configuration
- Oracle guest configuration
- common configuration (NTP settings, timezone)

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 on the PM&C server: `/var/TKLC/smac/guest-dropin/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.

Note: Change only those parameters that are marked in italics. Do not change the rest otherwise DIH installation may fail.

```
host,tvoe_hostname,172.16.1.1,TVOE,pic,255.255.255.248,
host,tvoe_hostname,tvoe_external_IP,TVOE,cust,tvoe_external_netmask,tvoe_external_gateway
host,oracle_hostname,172.16.1.2,ORACLE,pic,255.255.255.248,
host,oracle_hostname,oracle_external_IP,ORACLE,cust,oracle_external_netmask_,oracle_external_gateway
host,ixp_hostname,IXP-PDU,pic,172.16.1.3,255.255.255.248,,cust,ixp_external_IP,
ixp_external_netmask,ixp_external_gateway
host,nsp_hostname,172.16.1.5,NSP_DIH,pic,255.255.255.248,
host,nsp_hostname,nsp_external_IP,NSP_DIH,cust,nsp_external_netmask,nsp_external_gateway
```

```
bridge,cust,,DIH_external_interface
bridge,pic,,
bridge,monitor0,promisc,eth21
bridge,monitor1,promisc,eth22
ntpserver1,IP_address
ntpserver2,IP_address
nspprimary,172.16.1.5
nspsecondary,172.16.1.5
nsporacle,172.16.1.2
ixporacle,172.16.1.2
timezone,time_zone
```

Note: The following `host` record is a single line. There is no white-space. The text has been wrapped for its readibility.

```
host,ixp_hostname,IXP-PDU,pic,172.16.1.3,255.255.255.248,,cust,ixp_external_IP,ixp_external_netmask,ixp_external_gateway
```

Refer to the following descriptions of each keyword and its associated values.

`host` description (TVOE)

```
host,tvoe_hostname,172.16.1.1,TVOE,pic,255.255.255.248,
host,tvoe_hostname,tvoe_external_IP,TVOE,cust,tvoe_external_netmask,tvoe_external_gateway
```

Example:

```
host,tvoe,172.16.1.1,TVOE,pic,255.255.255.248,
host,tvoe,10.240.5.46,TVOE,cust,255.255.255.0,10.240.5.1
```

The host keyword has the following associated values:

tvoe_hostname The hostname of the TVOE host server. Example: `tvoe`

tvoe_external_IP The external IP address of TVOE host. Example: `10.240.5.46`

tvoe_external_netmask The external netmask the TVOE host. Example: `255.255.255.0`

tvoe_external_gateway The external gateway of the TVOE host. Example: `10.240.5.1`

`host` description (Oracle)

```
host,oracle_hostname,172.16.1.2,ORACLE,pic,255.255.255.248,
host,oracle_hostname,oracle_external_IP,ORACLE,cust,oracle_external_netmask_,oracle_external_gateway
```

Example:

```
host,ora,172.16.1.2,ORACLE,pic,255.255.255.248,
host,ora,10.240.5.229,ORACLE,cust,255.255.255.0,10.240.5.1
```

The host keyword has the following associated values:

oracle_hostname The hostname of the Oracle guest. Example: `ora`

oracle_external_IP The external IP address of Oracle guest. Example: `10.240.5.229`

oracle_external_netmask The external netmask the Oracle guest. Example: `255.255.255.0`

oracle_external_gateway The external gateway of the Oracle guest. Example: `10.240.5.1`

`host` description (IXP)

```
host,ixp_hostname,IXP-PDU,pic,172.16.1.3,255.255.255.248,,cust,ixp_external_IP,
ixp_external_netmask,ixp_external_gateway
```

Note: The `host` record in this template is a single line. There is no white-space. The text has been wrapped for its readibility.

Example:

```
host,ixp1337-1a,IXP-PDU,pic,172.16.1.3,255.255.255.248,,cust,10.240.5.230,255.255.255.0,10.240.5.1
```

The host keyword has the following associated values:

ixp_hostname The hostname of the IXP guest in the standard IXP format ixp*NNNN-1a*. Example: `ixp0666-1a`

- *N* is numeric 0-9

ixp_external_IP The external IP address of IXP guest. Example: `10.240.5.230`

ixp_external_netmask The external netmask the IXP guest. Example: `255.255.255.0`

ixp_external_gateway The external gateway of the IXP guest. Example: `10.240.5.1`

`host` description (NSP)

```
host,nsp_hostname,172.16.1.5,NSP_DIH,pic,255.255.255.248,
host,nsp_hostname,nsp_external_IP,NSP_DIH,cust,nsp_external_nettmask,nsp_external_gateway
```

Example:

```
host,nsp,172.16.1.5,NSP_DIH,pic,255.255.255.248,
host,nsp,10.240.5.224,NSP_DIH,cust,255.255.255.0,10.240.5.1
```

The host keyword has the following associated values:

nsp_hostname The hostname of the NSP guest. Example: `nsp`

nsp_external_IP The external IP address of NSP guest. Example: `10.240.5.224`

nsp_external_netmask The external netmask the NSP guest. Example: `255.255.255.0`

nsp_external_gateway The external gateway of the NSP guest. Example: `10.240.5.1`

`bridge` description

```
bridge,cust,,DIH_external_interface
bridge,pic,,
bridge,monitor0,promisc,eth21
bridge,monitor1,promisc,eth22
```

Example:

```
bridge,cust,,bond0.3/bond0.10
bridge,pic,,
bridge,monitor0,promisc,eth21
bridge,monitor1,promisc,eth22
```

The bridge keyword has the following associated values:

DIH_external_interface A list of TVOE interfaces that are connected to monitored network delimited by `/`. Example: `bond0.3/bond0.10`

ntpserver Description

```
ntpserver1,IP_address
ntpserver2,IP_address
```

- `ntpserver1` is the first NTP server
- `ntpserver2` is the second NTP server

Example:

```
ntpserver1,10.250.32.10
ntpserver2,
```

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server.

NSP Description

```
nspprimary,172.16.1.5
nspsecondary,172.16.1.5
nsporacle,172.16.1.2
ixporacle,172.16.1.2
```

- `nspprimary` is the NSP server
- `nspsecondary` is the NSP server
- `nsporacle` is the Oracle server for the NSP
- `ixporacle` is the Oracle server for the IXP

timezone Description

```
timezone,time_zone
```

```
timezone,America/New_York
```

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 corresponding to the examples above will appear as follows:

```
host,tvoe,172.16.1.1,TVOE,pic,255.255.255.248,
host,tvoe,10.240.5.46,TVOE,cust,255.255.255.0,10.240.5.1
host,ora,172.16.1.2,ORACLE,pic,255.255.255.248,
host,ora,10.240.5.229,ORACLE,cust,255.255.255.0,10.240.5.1
host,ixp1337-1a,IXP-PDU,pic,172.16.1.3,255.255.255.248,,cust,10.240.5.229,255.255.255.0,10.240.5.1
host,nsp,172.16.1.5,NSP_DIH,pic,255.255.255.248,
host,nsp,10.240.5.224,NSP_DIH,cust,255.255.255.0,10.240.5.1
bridge,cust,,bond0.3/bond0.10
bridge,pic,,
bridge,monitor0,promisc,eth21
bridge,monitor1,promisc,eth22
ntpserver1,10.250.32.10
ntpserver2,
nspprimary,172.16.1.5
nspsecondary,172.16.1.5
nsporacle,172.16.1.2
timezone,America/New_York
```

Appendix B

Knowledge Base Procedures

Topics:

3.14.1 Backup Procedure for TPD based Application

This procedure will backup system files which can be used at a later time to restore a failed system

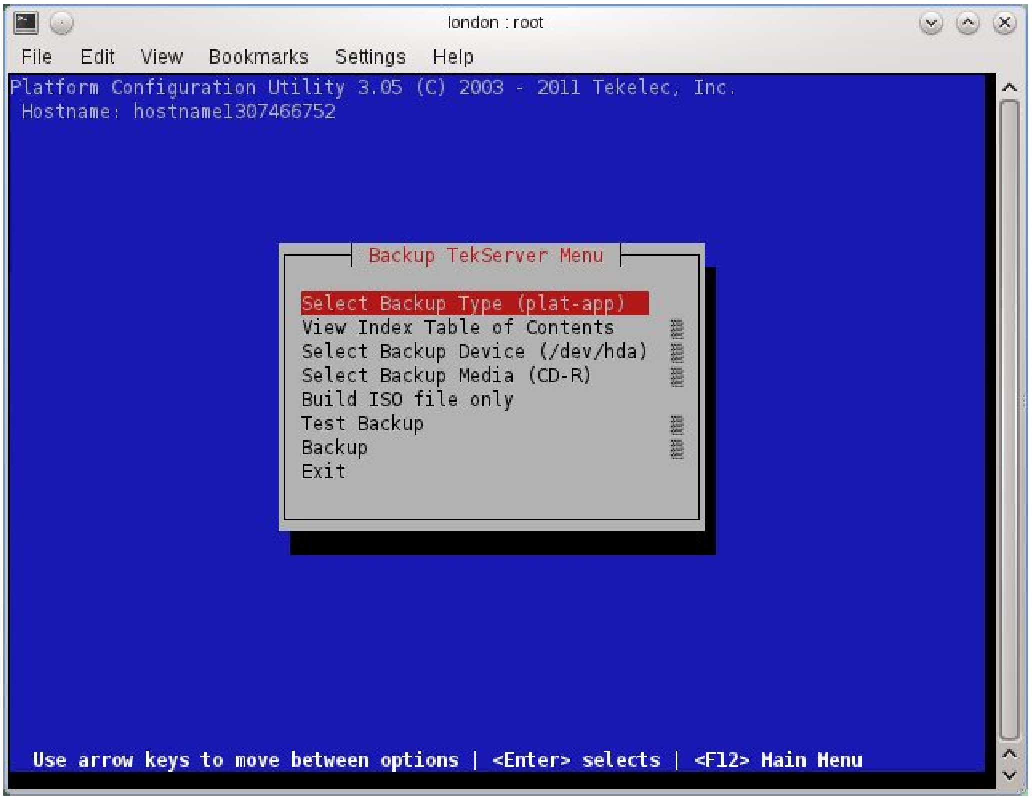
Note: The backup image is to be stored on a customer provided medium.

1. **TVOE Server:** Login as platcfg user.

   Login as platcfg user on the server. The platcfg main menu will be shown.

2. **TVOE Server:** Navigate to the Backup TekServer Menu page

   Select the following menu options sequentially: **Maintenance ➤ Backup and Restore ➤ Backup Platform (CD/DVD)**. The 'Backup TekServer Menu' page will now be shown.

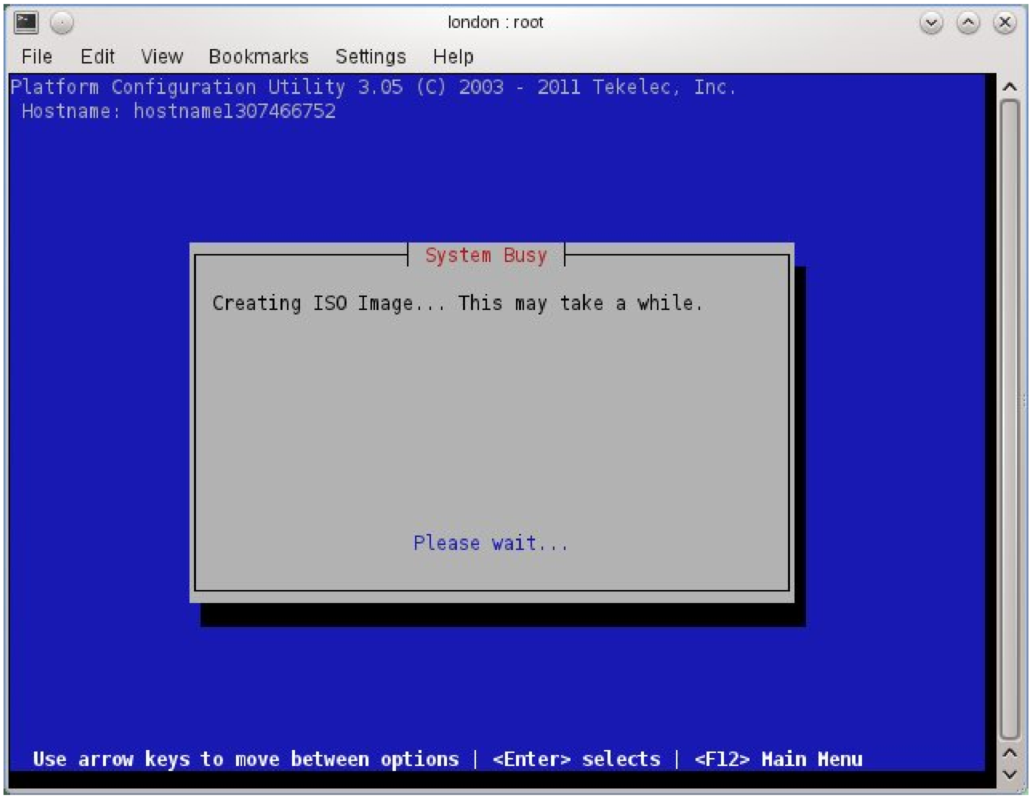


```
Platform Configuration Utility 3.05 (C) 2003 - 2011 Tekelec, Inc.
 Hostname: hostname1307466752

              Backup TekServer Menu

           Select Backup Type (plat-app)
           View Index Table of Contents
           Select Backup Device (/dev/hda)
           Select Backup Media (CD-R)
           Build ISO file only
           Test Backup
           Backup
           Exit

  Use arrow keys to move between options | <Enter> selects | <F12> Main Menu
```

3. **Server:** Build the backup ISO image.

   Select **Build ISO file only**. The following screen will display:

   Note: Creating the ISO image may happen so quickly that this screen may only appear for an instant.



```
Platform Configuration Utility 3.05 (C) 2003 - 2011 Tekelec, Inc.
 Hostname: hostname1307466752

System Busy

Creating ISO Image... This may take a while.

Please wait...

Use arrow keys to move between options | <Enter> selects | <F12> Main Menu
```

After the ISO is created, platcfg will return to the Backup TekServer Menu as shown in step 2. The ISO has now been created and is located in the `/var/TKLC/bkp/` directory. An example filename of a backup file that was created is: "hostname1307466752-plat-app-201104171705.iso"

4. **TVOE Server:** Exit platcfg

   Select **Exit** on each menu until platcfg has been exited. The SSH connection to the TVOE server will be terminated.

5. **PM&C Server:** Copy backup image to the customer system where it can be safely stored

   If the customer system is a Linux sytem, please execute the following command to copy the backup image to the customer system.

   ```
   # scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/
   ```

   When prompted, enter the tvoexfer user password and press **Enter**.

   An example of the output looks like:

   ```
   # scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/
   tvoexfer@10.24.34.73's password:
   hostname1301859532-plat-app-301104171705.iso     100% 134MB 26.9MB/s 00:05
   ```

   If the Customer System is a Windows system please refer to Appendix A Using WinSCP to copy the backup image to the customer system.

   The TVOE backup file has now been successfully placed on the Customer System.

Appendix C

Installation Procedure for Second DIH Enclosure

Topics:

Create External Bulkconfig File

Create the bulkconfig file

a) Open a terminal window and log in to PM&C server as root.

b) Create the /var/TKLC/smac/guest-dropin/bulkconfig file.

The pic bridge should be associated with the IMI network.

The bonded interface vlan tag should match the IMI vlan id.

Example: bridge, pic, bond0.4

The example pic network address works, however it can be changed as needed.

```
host,demo1,172.16.1.6,TVOE,pic,255.255.255.224,
host,ora,172.16.1.7,ORACLE,pic,255.255.255.224,
host,ora,10.240.30.12,ORACLE,cust,255.255.255.224,10.240.30.3
host,ixp1337-1a,IXP
PDU,pic,172.16.1.8,255.255.255.224,,cust,10.240.30.13,255.255.255.224,10.240.30.3
host,nsp,172.16.1.5,NSP_DIH,pic,255.255.255.224,
host,demo1,10.240.30.10,TVOE,cust,255.255.255.224,10.240.30.3
host,nsp,10.240.30.11,NSP_DIH,cust,255.255.255.224,10.240.30.3
bridge,cust,,bond0.3
bridge,pic,,bond0.4
bridge,monitor0,promisc,eth21
bridge,monitor1,promisc,eth22
ntpserver1,10.250.32.10
ntpserver2,10.240.30.3
nspprimary,172.16.1.5
nspsecondary,172.16.1.5
nsporacle,172.16.1.2
ixporacle,172.16.1.7
timezone,America/New_York
```

Note: nsporacle should be the ip address of the remote oracle server.

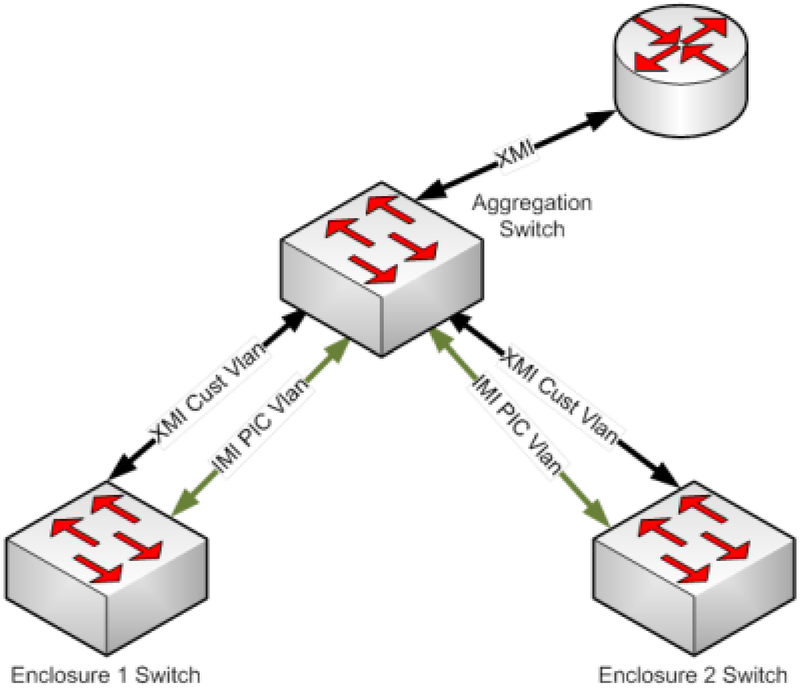


Figure 1: Dual Instance of IXP and PMF

c) Replace all DIH 172 addresses with the IMI addresses in the bulk configuration file as needed.

Configure TVOE Host Performance (BIOS)

1. Enter host server BIOS setup utility
   a) Reboot the server
   b) As computer boots, press **F9** to access the BIOS setup utility and press **Enter**.
2. Disable hyperthreading
   a) Select **System Options** and press **Enter**.
   b) Select **Processor Options** and press **Enter**.
   c) Select **Intel Hyper threading Options** and press **Enter**.
   d) Select **Disable** and press **Enter**.
3. Enable maximum performance
   a) Select **Power Management Options** and press **Enter**.
   b) Select **HP Power Profile Options** and press **Enter**.
   c) Select **Maximum Performance** and press **Enter**.
4. Exit BIOS
   a) Press **Esc** to exit the utility.
   b) Press **F10** to confirm the exit from the utility.

Install Operating System on TVOE host

1. Login
   a) If needed, open web browser and enter:
      - **http://<management_network_ip>**

   b) Login as **pmacadmin** user.
2. Navigate to Software Inventory
   a) Navigate to **Main Menu**>**Software**>**Software Inventory**.
3. Select servers
   a) Select the server you want to IPM. Then press the **Install OS** button.
4. Initiate OS Install
   a) Then press the **Start Install** button.
5. Monitor OS Install
   a) Navigate to **Main Menu** >**Task Monitoring** to monitor the progress of the OS Installation

Configure TVOE Host

1. Configure the TVOE host server hostname.
   a) Open a web browser and log in to the TVOE host blade iLO.
   b) Open a virtual console and log in to the TVOE host blade as root.
   c) Navigate to platcfg. As root run:
      - **# su - platcfg**

   d) Navigate to **Server Configuration** > **Hostname**.
   e) Click **Edit** and enter the TVOE server hostname, the same that was previously set in the DIH
   f) Common Bulkconfig file. Save the changes and exit the platcfg menu.
2. Configure SNMP on TVOE host.
   a) Connect on TVOE system as platcfg
   b) Go to **Network Configuration** > **SNMP configuration** > **NMS Configuration**.
   c) Add One Destination per guest.
      - Select **Edit** > **Add a new NMS server**.
      - Enter IP (Internal IP of NSP server), port=162 and community=TEKELEC
      - Select **OK**

   d) Confirm restart of Alarm Routing Service when exiting Edit.
   e) Exit
3. Run TVOE bulk configuration (PM&C console).
   a) Open a terminal window and log in to the PM&C server as root.

b) Verify Designation and Function are set via the Platform configuration Menu before running the bulk configuration script.
If it is not set please set Designation to 1A and Function to PMAC.

c) Locate the directory where the imported IXP ISO is mounted. As root run:

- **# ls -ld /usr/TKLC/smac/html/TPD/IXP***

d) Locate the directory with the proper IXP version.

e) Run the TVOE configuration using the bulkConfig.pl script from the IXP ISO. As root run:

- **# /usr/TKLC/smac/html/TPD/IXP--ixp_version--i386/upgrade/lib/bulkConfig.pl --tvoe tvoe_host_control_ip -f /var/TKLC/smac/guest-dropin/bulkconfig** where *ixp_version* is the version of the IXP application and *tvoe_host_control_ip* is the TVOE control network IP address.
- Example: **#/usr/TKLC/smac/html/TPD/IXP--8.0.0_2.2.0--872-2268-101--i386/upgrade/lib/bulkConfig.pl --tvoe 169.254.116.194 -f /var/TKLC/smac/guest-dropin/bulkconfig**
- **Note:** The script will pause and expect the user to login to the TVOE host. Provide the root userid and password for the TVOE machine for the script to continue.

Create Guests

The guest profile names are:

- ixp for IXP application
- ora for Oracle application
- pmf for PMF application

1. Navigate to VM entities list

a) Open a web browser and log in to the PM&C application interface as `pmacadmin`.

b) Navigate to VM Management.

c) A VM entities list will appear. Click on particular TVOE host blade server (identified by Enc:*id*, Bay:*id*).

2. Create guest

a) Click on Create Guest.

b) Click on Import Profile.

c) Select the profile under the ISO/profile drop-down menu.

d) Click on Select Profile.

e) Click on Create. Monitor the progress of guest creation. Check that the guest has been created successfully.

Note: Repeat this step for all 3 profiles (ixp, ora, pmf) to create 3 guests.

IPM Guests

The guest profile names are:

- ixp for IXP application
- ora for Oracle application
- pmf for PMF application

Install TPD on guest

a) Open a web browser and log in to the PM&C application interface as `pmacadmin`.
b) Navigate to VM Management
c) A VM entities list will appear. Click on particular TVOE host blade server (identified by Enc:*id* Bay:*id*
d) A sublist with guests will appear. Click on a particular guest.
e) Click on Install OS. A list of available TPD ISOs will appear.
f) Select a particular TPD and click on Start Install.
g) Observe Task Monitoring page for installation progress. Wait until the operation system is installed. Check status that the operation system has been installed successfully.

Note: Repeat this procedure for all 3 guests.

Install Oracle Guest

1. Login to Oracle guest and set hostname.

a) On the TVOE host, open the ora console.

- # virsh console ora

b) Enter the platcfg menu. As root run:

- **# su - platcfg**

c) Navigate to **Server Configuration** > **Hostname**. Click **Edit** and set the server hostname. Exit the platcfg menu.

2. Install Oracle from PM&C GUI

a) Open a web browser and log in to the PM&C application interface as `pmacadmin`.
b) Navigate to **VM Management**.
c) A VM entities list will appear. Click on particular TVOE host blade server (identified by Enc:*id* Bay:*id*).
d) A sublist with guests will appear. Click on a particular guest.
e) Click on **Upgrade**. A list of available ISOs will appear.
f) Select a particular application ISO and click on **Start Upgrade**. An application upgrade will be triggered.
g) Observe **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Check status that the application has been upgraded successfully.

3. Configure Oracle

a) Log back to rebooted guest as root.

b) Configure Oracle. As root run:

- # **/opt/dih/configureOracle.sh**

c) Wait until the Oracle configuration will finish.

4. Run Oracle Health Check

a) Open a terminal window and log in to Oracle guest as grid user.

b) As grid run:

- $ **crsctl status resource -t**

c) Once the Oracle stack has fully started, the output should be as follows where the STATE_DETAILS of the database resource (ora.pic.db) equals "Open".

```
-----------------------------------------------------------------------------
NAME           TARGET  STATE        SERVER                   STATE_DETAILS
-----------------------------------------------------------------------------
Local Resources
-----------------------------------------------------------------------------
ora.DATA.dg
ONLINE  ONLINE       ora
ora.LISTENERASM.lsnr
ONLINE  ONLINE       ora
ora.asm
ONLINE  ONLINE       ora                      Started
ora.ons
ONLINE  ONLINE       ora
-----------------------------------------------------------------------------
Cluster Resources
-----------------------------------------------------------------------------
ora.cssd
1        ONLINE  ONLINE       ora
ora.diskmon
1        ONLINE  ONLINE       ora
ora.evmd
1        ONLINE  ONLINE       ora
ora.pic.db
1        ONLINE  ONLINE       ora                      Open
```

Install IXP Guest

1. Login to IXP guest and set hostname.

a) On the TVOE host, open the ixp console.

- **# virsh console ixp**

b) Enter the platcfg menu. As root run:

- # **su - platcfg**

c) Navigate to **Server Configuration** > **Hostname**. Click **Edit** and set the server hostname.

Note: Match the hostname to bulkconfig file

d) Exit the platcfg menu.

2. Install IXP from the PM&C GUI

a) Open a web browser and log in to the PM&C application interface as `pmacadmin`.
b) Navigate to **VM Management**.
c) The VM entities list will appear. Click on particular TVOE host blade server (identified by Enc:*id* Bay:*id*).
d) A sublist with guests will appear. Click on a particular guest.
e) Click on **Upgrade**. A list of available ISOs will appear.
f) Select a particular application ISO and click on **Start Upgrade**. An application upgrade will be triggered.
g) Observe **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Verify application has been upgraded successfully.
h) After task completion, IXP will reboot.

3. Finalize IXP guest installation

a) Run as root:
# **installIXP**
b) Wait until installation script completes, there should be no errors in the script output.
c) If there are any errors, contact the Tekelec Customer Care Center.

4. Post-install Oracle Configuration

a) Open a terminal window and log in to DIH IXP PDU Storage server as root.
b) Run DIH Oracle configuration. As root run:

- # **cd_oracle_utils**
- # **./oracle-postinstall.pl -auto -conn=system/manager@ixp_oracle/pic -connsys=sys/oracle@ixp_oracle/pic**

c) When the script finishes, check the log file /var/TKLC/log/ixp/postinstall-oracle.log for errors.
d) If there are any errors, contact the Tekelec Customer Care Center.
e) Example output:

```
--CUT--
inf | --- Calculated new sizing in space usage:
inf | part | existing | requested | target
inf | Temp size | 12884901888 | 17179869184 | as requested
inf | DATA_CDR size |137438953472 |1272487125741 | 1271310319616
inf | DATA_IND size | 34359738368 |1040365377590 | 1030792151040
inf |oraindex DATA_CDR size | 0 | 289237746768 | 274877906944
inf | --- Calculated new sizing in number of files:
inf | part | exists |requested| create | cdr:ind %
inf | Temp files | 6 | 8 | 2 | na
inf | DATA_CDR data | 8 | 74 | 66 | 48.879
inf | DATA_IND data | 2 | 60 | 58 | 39.632
inf |oraindex DATA_CDR data | 0 | 16 | 16 | 10.569
war | Will create 2 temp files.
war | Will create 66 DATA_CDR data files.
war | Will create 58 DATA_IND data files.
war | Will create 16 DATA_CDR data files at oraindex.
inf | File: 0/142 at 1GB avg 0.00s, ETA 0.00s
inf | File: 1/142 at 1GB avg 0.00s, ETA 0.00s
inf | File: 2/142 at 1GB avg 0.00s, ETA 0.00s
inf | File: 3/142 at 1GB avg 3.69s, ETA 8201.00s
inf | File: 4/142 at 1GB avg 3.69s, ETA 8145.94s
inf | File: 5/142 at 1GB avg 3.70s, ETA 8111.01s
inf | File: 6/142 at 1GB avg 3.70s, ETA 8057.48s
inf | File: 7/142 at 1GB avg 3.71s, ETA 8014.10s
inf | File: 8/142 at 1GB avg 3.72s, ETA 7969.14s
--CUT—
```

5. IXP Post-Install Healthcheck

a) As cfguser, run:

- $ **analyze_server.sh -p**

b) Analyze the output of the script for any errors. Issues reported by this script must be resolved.

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

- Example of overall output:

```
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.

Install PMF Guest

1. Login to PMF guest and set hostname.

a) On the TVOE host, open the pmf console.

- **# virsh console pmf**

b) Enter the platcfg menu. As root run:

- # **su - platcfg**

c) Navigate to **Server Configuration** > **Hostname**. Click **Edit** and set the server hostname.

- ext-0a

d) Exit the platcfg menu.

2. Install PMF from PM&C GUI.

a) Open a web browser and log in to the PM&C application interface as `pmacadmin`.
b) Navigate to **VM Management**.
c) The **VM entities** list will appear. Click on particular TVOE host blade server (identified by Enc:*id* Bay:*id*).
d) A sublist with guests will appear. Click on the pmf guest.
e) Click on **Upgrade**. A list of available ISOs will appear.
f) Select the xmf application ISO and click on **Start Upgrade**.
g) Observe **Task Monitoring** page for upgrade progress. Wait until the upgrade is finished. Verify application has been upgraded successfully.

3. Configure PMF network.

a) As root on PMF run:

- # **netAdm set --address=172.16.1.9 --netmask=255.255.255.224 --device=pic**
- # **su - platcfg**
- Navigate to**Network Configuration** >**Modify Hosts File**. Click**Edit** and Edit Alias.
- **Select cust0-a entry** and change pmf-0a to ext-0a
- Exit the platcfg menu.
- #su - cfguser -c "prod.start -C"
- #reboot

4. xMF Post-Install Healthcheck

a) As cfguser, run:

- $ **analyze_server.sh -p**

b) Analyze the output of the script for errors. Issues reported by this script must be resolved.
c) 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
```

IMI Address Configuration

Perform this task, only if the DIH addresses were changed to the IMI addresses in the *Create External Bulkconfig File*

1. netAdm set-address=x.x.x.x-netmask=255.255.255.x-device=pic
2. Navigate to **Network Configuration ➤ Modify Hosts File**. Click Edit and Delete Host.
3. Select cust0-a entry
   a) Click Yes
4. Select Delete Host
5. Select appserver entry
   a) Click Yes
6. Select Delete Host
7. Select ntpserver1 entry
   a) Click Yes
8. Select Add Host
   a) x.x.x.x (IMI pmf-0a IP address)
   b) cust-0a
   c) Click Yes
9. Select Add Host
   a) x.x.x.x (IMI nsp IP address)
   b) appserver
   c) Click Yes
10. Select Add Host
    a) x.x.x.x (IMI tvoe address)
    b) ntpserver1
    c) Click Yes
11. Select Add Alias
    a) Select cust-0a
    b) Enter new alias: pmf-0a
12. Exit the platcfg menu
13. #su - cfguser-c" prod.start-C
14. #reboot

Creating an External DWH

Prior to proceeding with the DIH Post-Install Configuration step, an external DWH must be created and used when creating the second IXP subsystem in Equipment Registry.

1. Log into the NSP application.
   a) Log in as user "tekelec" to the NSP application interface using the NSP IP address.
   b) Click Centralized Configuration.
   The NSP application launches.
2. Create a site on NSP.
   a) Select **Equipment Registry ➤ Sites ➤ Add**
   b) Type the desired site name and click Add. A typical name might be DWHRemoteSite.
3. Add the external DWS on the NSP.
   a) Select **Equipment Registry ➤ Sites New site previously created ➤ DWH Add**
   b) Type the desired name for the new DWH. A typical name might be DIH_IXP_STORAGE_ENC2.
   c) Leave version at default value.
   d) Enter Login User Id as IXP.
   e) Enter Password as IXP.
   f) Enter Service Name as PIC.
   g) Leave Port as default value 1521.
   h) For the IP Address use the DIH address defined in the second enclosure bulkconfig for ora.
   i) Click Add.
   j) Note the banner instructing the user to apply changes on the existing IXP subsystem. Apply changes.

Summary

Having installed a second DIH enclosure, proceed to section *DIH Post-Install Configuration*.

All steps should be executed except steps 1, 2, and 4 in section *Install xDR Builders*.

Appendix D

Bond Creation

Topics:

Bond Creation

1. Login as root on TVOE
2. Execute the command `# su - platcfg`
3. Go to the menu --> **Network Configuration** --> **Network Interfaces** --> **Add an Interface** --> **Add New Interface**
4. Select Bonded

   (*) Bonded
5. Select interfaces to enslave
   - **eth21: ( ) (*) bond interface**
   - **eth22: ( ) (*) bond interface**
6. Select **OK**
7. Once complete, exit platconfig menu
8. Rreboot the TVOE host and be sure to add bond1 interface to the bulk configuration file as line: **bridge,cust,,bond1**

Glossary

A

A

Ampere

Association

An association refers to an SCTP association. The association provides the transport for protocol data units and adaptation layer peer messages.

C

CD

Carrier Detect

Compact Disk

Call Deflection

Configuration

Dynamic and shorter-term management tasks. These include modifications to parameters. This term is often used interchangeably with provisioning.

D

disk

A single disk drive residing in a Controller Enclosure or a Disk Enclosure. A Disk can be assigned to a Disk Group, designated as a Spare or Global Spare, or left unused.

DVD

Digital Versatile Disk

F

frame

A frame is a floor mounted cabinet which may house a variety of equipment to provide communications processing and connectivity. It is constructed from channel steel and painted with electrostatic powder. Each cabinet may include top and side panels as

F

well as a door. The cabinet provides adequate air flow, as well as front and rear access for cabling and equipment replacement. Cable management is provided by overhead trays and underneath the frame (when the frame is mounted on a raised floor). It can be configured for AC or DC applications. Frames are typically 7-feet tall and may be 19-inch or 23-inch wide cabinets depending upon product family.

G

GB

Gigabyte — 1,073,741,824 bytes

GUI

Graphical User Interface

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

I

IP

Internet Protocol

IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

ISO

International Standards Organization

I

IXP

An Intel network processor used on the HIPR card.

N

NSP

Network Services Part

The lower layers of the SS7 protocol, comprised of the three levels of the Message Transfer Part (MTP) plus the signaling Connection Control Part (SCCP), are known collectively as the Network Services Part (NSP).

P

PM

Processing Module

PM&C

Platform Management and Configuration

Server with hardware management software that manages the remaining servers (System OAMs and MPs) in a network element. The terms PM&C and system manager are used synonymously in the online help documentation. PM&C functions include hardware monitoring and control, switch configuration, and software installation and upgrade.

Provides hardware and platform management capabilities at the site level for Tekelec platforms. The PMAC application manages and monitors the platform and installs the TPD operating system from a single interface.

R

RAM

Random Access Memory

A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes.

R

removable media

Flash memory or “thumb” drives used in the latched USB port on an E5-MCAP card for installation and backup of customer data.

S

SCP

Service Control Point

Service Control Points (SCP) are network intelligence centers where databases or call processing information is stored. The primary function of SCPs is to respond to queries from other SPs by retrieving the requested information from the appropriate database, and sending it back to the originator of the request.

Secure Copy

server

Any computer that runs TPD. Could be a Rack Mount Server or a Blade Server.

SSH

Secure Shell

A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE 5 ISS IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

T

TPD

Tekelec Platform Distribution

TPD is a standard Linux-based operating system packaged and distributed by Tekelec. TPD provides value-added features for managing installations and upgrades, diagnostics, integration of 3rd party software (open and

T

	closed source), build tools, and server management tools.

U

URL	Uniform Resource Locator