Oracle® Communications
Integrated Diameter Intelligence Hub

IDIH 6.X Installation Guide

Release 6.0

E56571-05

Aguest 2016

ORACLE®

Oracle Communications IDIH 6.x Installation Guide, Release 6.0

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.
Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

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

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

See more information on MOS in the Appendix section.

Table of Contents

Chapter 1

Introduction

Topics:

1.1 IDIH

Integrated Diameter Intelligence Hub is a diameter troubleshooting application, scoped to integrate with one DSR and one geographical site. IDIH provides the ability to troubleshoot diameter traffic. Diameter traffic is captured by applying filters on DSR. Integrated Diameter Intelligence Hub is comprised of three guests running on a TVOE host, which are Oracle, Mediation and Application guests. Sections 1.2 through 1.4 describe these guests.

1.2 Oracle Guest

The Oracle Guest hosts the Oracle database for storing configuration and Diameter trace data. The Oracle Guest persists TTRs, TDRs and Trace Statistics for long term. The Oracle Guest Supports APIs for searching through TTRs, TDRs and Trace Statics. It holds schema configuration parameters responsible for management of data partitions, data retention and table truncation.

1.3 Mediation Guest

The Mediation Guest is responsible for communicating with DSR and processing Diameter trace data. The Mediation Guest hosts the DSR ComAgent interface which allows it to receive TTRs for a Trace. The Mediation Guest processes Diameter TTRs and translates them to a human readable format, known as a TDR, which allows business applications to search and filter the trace data. The Mediation Guest provides the statistics module for generating statistics for each of the Traces. Hosts interface to the Database Server for storing TTRs, TDRs and Trace Statistics.

1.4 Application Guest

The Application Guest is used as the visualization interface for the end user. It hosts Business applications like Protrace for visualizing the Trace Statistics, Traces and Ladder Diagrams. The Application Guest provides operations, administration and management interface for IDIH. The Application Guest encapsulates the workflow enabling users to perform Diameter troubleshooting. It initiates the SOAP service calls to DSR which populate DSR Configuration Data in the IDIH. The Application Guest uses DSR configuration data at the time of visualization for mapping trace diameter data and metadata into meaningful names and entities.

1.5 Deployment Tools

fdconfig is the command-line tool used to automatically deploy and configure the TVOE host, Oracle Guest, Mediation Guest, and Application Guest. fdconfig requires the presence of an initialized PM&C to perform the steps necessary for deployment and configuration. The fdconfig program is to be run on the PM&C server itself. The following use cases demonstrate typical functions:

- The "site manager" updates the PM&C Hardware Repository in order to:
  1. Add or delete infrastructure element credentials in the repository.

2. Update passwords

- The "system administrator or installer" uses configuration files to execute deployment and configuration procedures on target devices. These activities include:
  1. Provision cabinets, enclosures and rack-mount servers in PM&C
  2. Install TVOE hosts
  3. Create TVOE guests
  4. Install application guests or native application servers
- The "system administrator" creates configuration files that describe the infrastructure into which the application servers will be installed. This is done to:
  1. Describe PM&C interfaces (SOAP and SCP)
  2. Describe available hardware
  3. Describe hosts, guests and native application installations and configurations

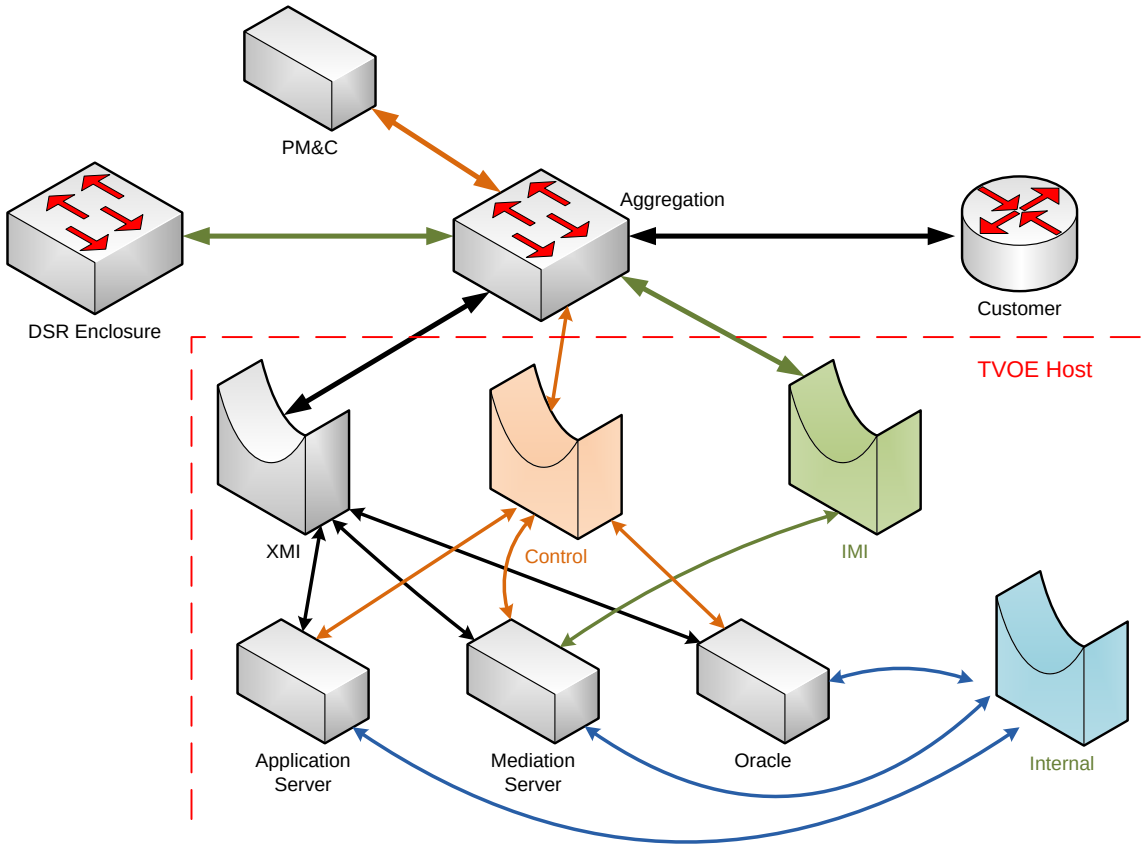
The fdconfig configuration file (FDC) is an XML file of well-defined format. The configuration file is provided to the fdconfig program at deployment time.

Chapter 2

Network Configuration

Topics:

2.1 Network



The Integrated Diameter Intelligence Hub utilizes four networks to operate, they are the control network, xmi network, imi network and the internal network. The xmi network is used to provide a web interface to the end user. The imi network provides the ComAgent data feed from the DSR to the IDIH mediation server. The internal network provides a means for the three guest to communication internally. The control network is used to provision the IDIH via PM&C. These networks are described in more detail in sections 2.2 through.

2.2 Network Bridges

Four bridges are required for IDIH, however only three of the bridges use physical interfaces. The internal bridge does not use a physical interface.

- Two to six network interfaces can be used to configure the IDIH network, this is dependent on customer requirements. Two interfaces on a single bond with multiple VLAN tags are sufficient. However some customers prefer to have the networks isolated at the hardware level if that is the case you simply configure separate interfaces for the xmi and imi bridges.

2.3 XMI Network

External Management Network

- The External Management Network is used to access the Application server GUI, and to service the various guest as needed through ssh or the dbconsole in the case of the oracle server. It also

provides access to a remote time source. In the case where an engineer intends to install IDIH on a pre-existing PM&C that has the management bridge setup on the xmi network, the engineer can simply rename the xmi interface the management interface. The following is a list of the service and their port numbers:

- Application Web Interface
    - Port 80 and 443
- Oracle Console
    - Port 1158
- Secure Shell
    - Port 22
- NTP
    - Port 123

XMI Bridge

- Typically bond0 VLAN tagged
    - Example: bond0.3

2.4 IMI Network

Internal Management Network

- The Internal Management Network is used as the data feed from the DSR system to the Mediation guest and for communication between the mediation guest and the DSR system specifically Service Mix and the ComAgent.
    - Service Mix
        - Port 8282
    - ComAgent
        - Port 16529

IMI Bridge

- Typically a bond1 VLAN tagged interface.
    - Example: bond1.4

2.5 INT Network

Internal Network

- The internal network provides a means for the IDIH applications to communicate amongst each other. The Internal network is used to access the oracle database via the mediation and application guests. In addition Alarm traffic sent to the application via this network. I have not listed the port numbers for the services since this network is internal to the TVOE host.
    - Application Database Query
    - Oracle Database Traffic
    - Mediation Traffic
    - Secure Shell Access
    - Alarms

2.6 Control Network

Application deployment

Control Bridge

- The control bridge is setup on the TVOE host during IPM. There is no action needed by the installation team where it concerns IDIH. I have not listed the ports as this network is internal to the DSR, PM&C and IDIH.
    - Secure Shell Access
    - NFS
    - Kickstart
    - PM&C TVOE proprietary deployment

2.7 Network Hardware Configuration

- One of the first steps in the IDIH installation process is to record your intended network and hardware architecture. We have pre-defined FDC templates for each of the installation scenarios. We have broken it down to five hardware scenarios and each of these have two network scenarios. If you have XMI, IMI and control networks isolated on separate switch pairs then you would need a Multi-uplink configuration. If you have XMI, IMI and control networks available on a single switch pair then you should choose the single uplink configuration.
    - Hardware
        - HP and Netra IDIH RMS with PMAC
            - Single Uplink
            - Multiple Uplink
        - HP and Netra IDIH RMS stand-alone
            - Single Uplink
            - Multiple Uplink
        - IDIH Blade
            - Single Uplink
            - Multiple Uplink
- We have provided example forms in this section for each scenario, they are fully populated examples, in Appendix D you can find ten forms that correlate to the ten scenarios. There are ten different FDC files available and they represent each of the scenarios we present in the installation document.

- When installing rack mount servers you must provide the ILO IP address, in the case of a blade installation you would provide the OA ip addresses, enclosure id and bay that contains the IDIH TVOE host. IDIH installations that co-exist with a PM&C are only supported on RMS hardware.

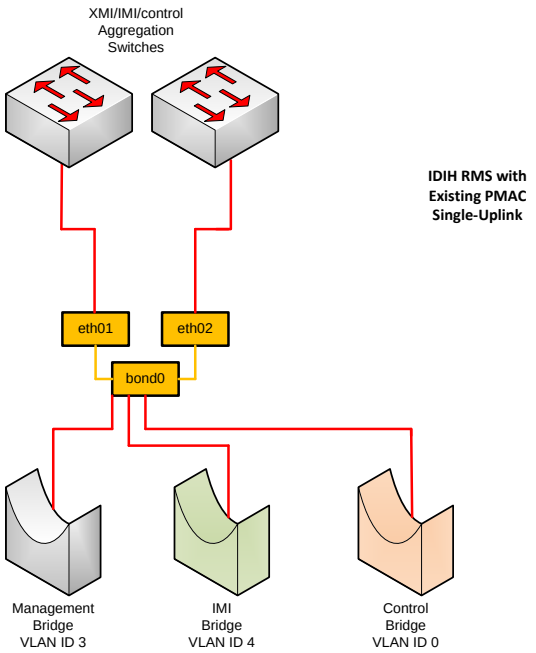
- The bond1 interface configuration is automated with Fast Deployment, there is no need to preconfigure the bond1 interface, simply follow the Multiple Uplink form and provide the interfaces you intend enslave in bond1, typically eth03,eth04 on RMS and eth21, eth22 on Blades. However you don't have to use eth03,eth04 for RMS you could use eth05, eth06 etcetera. This holds true for blades as well, you could use ports eth11,eth12 or eth21,eth22 for the Blade. This is dependent on the switch and enclosure configuration that the customer has on site. Simply replace the template values with the interfaces that you need.

2.8 HP and Netra IDIH RMS Installation with PMAC

Note: Values enclosed with angle brackets <>, should be modified for your installation.

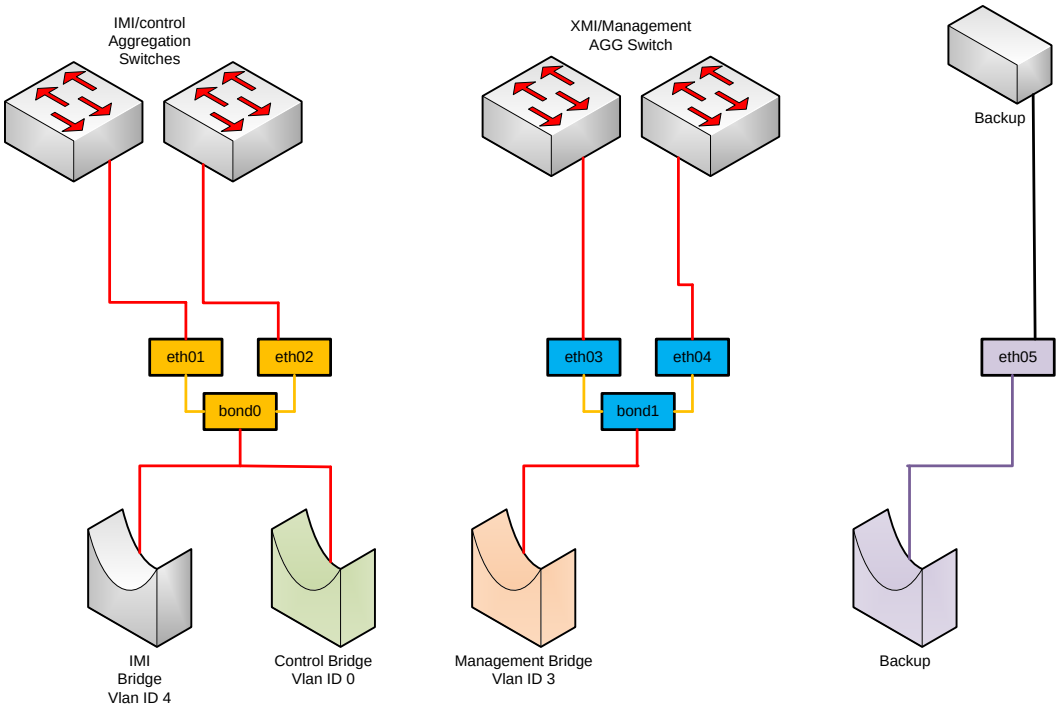
- **Rack-mount Server element**
  RMS ID: mgmtsrvr ILO Address: <10.250.36.27> RMS name: <atl-tvoe>
  Cabinet HW ID: <cab1>
- **TVOE Host element**
  TVOE host ID: mgmtsrvrtvoe RMS Hardware ID: mgmtsrvr TVOE hostname: <atl-tvoe>
- **NTP servers**
  ntpserver1 IP: <10.250.32.10> ntpserver2 IP:

- **RMS Single-Uplink (Bond0) with PMAC**
  - Config File Options: idihRmsPmacSingle.xml



- **TVOE Management interface**
  Device: <bond0.3> VLAN ID: <3>
- **TVOE IMI interface**
  Device: <bond0.4> VLAN ID: <4>
- **TVOE Management Bridge**
  Interface: <bond0.3> IP Address: <10.250.51.39> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **TVOE IMI Bridge**
  Interface: <bond0.4>
- **Oracle Guest Hostname:** <atl-ora>
  Management IP Address: <10.250.51.184> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **Mediation Guest Hostname:** <atl-med>
  Management IP Address: <10.250.51.185> Netmask: <255.255.255.0> gateway: <10.250.51.1>
  IMI IP Address: <192.168.10.55> Netmask: <255.255.255.0>
- **Application Guest Hostname:** <atl-app>
  Management IP Address: <10.250.51.186> Netmask: <255.255.255.0> gateway: <10.250.51.1>

- **RMS Multi-Uplink (Bond0, Bond1, eth05) with PMAC**
  - **Config File Options:** idihRmsPmacMulti.xml



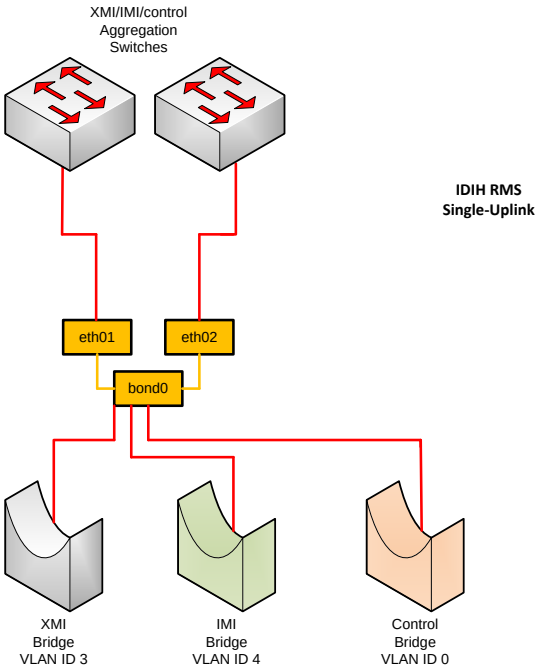
- **TVOE Management interface**
  Device: <bond1> Bond Interfaces : <eth03,eth04>
- **TVOE IMI interface**
  Device: <bond0.4> VLAN ID: <4>
- **TVOE Management Bridge**
  Interface: <bond1>IP Address: <10.250.51.39> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **TVOE IMI Bridge**
  Interface: <bond0.4>
- **Oracle Guest Hostname:** <atl-ora>
  Management IP Address: <10.250.51.184> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **Mediation Guest Hostname:** <atl-med>
  Management IP Address: <10.250.51.185> Netmask: <255.255.255.0> gateway: <10.250.51.1>
  IMI IP Address: <192.168.10.55> Netmask: <255.255.255.0>
- **Application Guest Hostname:** <atl-app>
  Management IP Address: <10.250.51.186> Netmask: <255.255.255.0> gateway: <10.250.51.1>

2.9 HP and Netra IDIH RMS Installation Stand-Alone

Note: Values enclosed with angle brackets <>, should be modified for your installation.

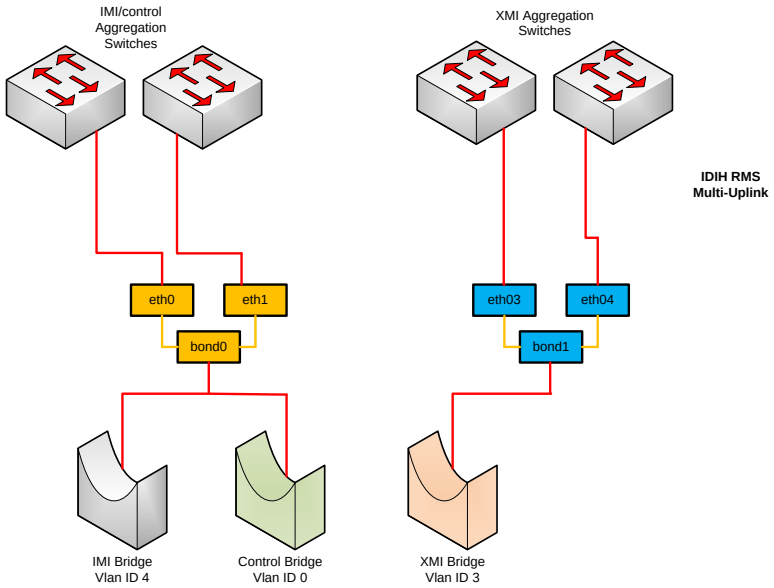
- **Rack-mount Server element**
  RMS ID: srvr ILO Address: <10.250.36.27> RMS name: <atl-tvoe> Cabinet HW ID: <cab1>
- **TVOE Host element**
  TVOE host ID: srvrtvoe RMS Hardware ID: srvr TVOE hostname: <atl-tvoe>
- **NTP servers**
  ntpserver1 IP: <10.250.32.10> ntpserver2 IP:

- **RMS Single-Uplink (Bond0) stand-alone**
  - **Config File Options:** idihRmsSingle.xml



- **TVOE XMI interface**
  Device: <bond0.3> VLAN ID: <3>
- **TVOE IMI interface**
  Device: <bond0.4> VLAN ID: <4>
- **TVOE XMI Bridge**
  Interface: <bond0.3> IP Address: <10.250.51.39> Netmask:<255.255.255.0> gateway: <10.250.51.1>
- **TVOE IMI Bridge**
  Interface: <bond0.4>
- **Oracle Guest Hostname:** <atl-ora>
  XMI IP Address: <10.250.51.184> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **Mediation Guest Hostname:** <atl-med>
  XMI IP Address: <10.250.51.185> Netmask: <255.255.255.0> gateway: <10.250.51.1>
  IMI IP Address: <192.168.10.55> Netmask: <255.255.255.0>
- **Application Guest Hostname:** <atl-app>
  XMI IP Address: <10.250.51.186> Netmask: <255.255.255.0> gateway: <10.250.51.1>

- **RMS Multi-Uplink (Bond0, Bond1) stand-alone**
  - **Config File Options:** idihRmsMulti.xml



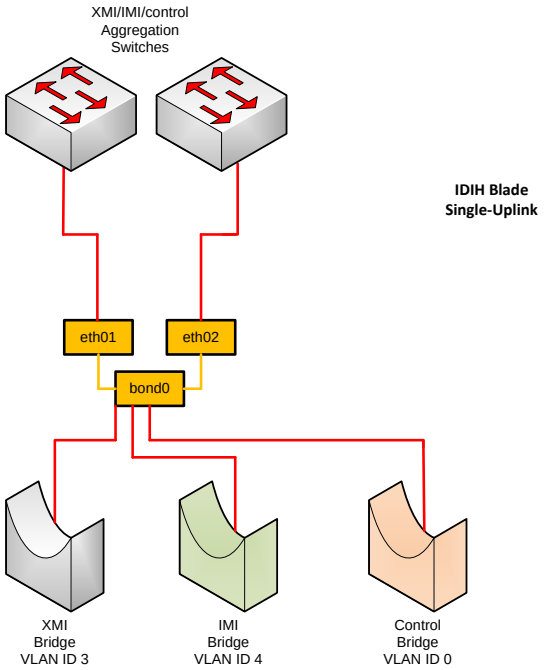
- **TVOE Management interface**
  Device: <bond1> Bond Interfaces : <eth03,eth04>
- **TVOE IMI interface**
  Device: <bond0.4> VLAN ID: <4>
- **TVOE XMI Bridge**
  Interface: <bond1> IP Address: <10.250.51.39> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **TVOE IMI Bridge**
  Interface: <bond0.4>
- **Oracle Guest Hostname:** <atl-ora>
  XMI IP Address: <10.250.51.184> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **Mediation Guest Hostname:** <atl-med>
  XMI IP Address: <10.250.51.185> Netmask: <255.255.255.0> gateway: <10.250.51.1>
  IMI IP Address: <192.168.10.55> Netmask: <255.255.255.0>
- **Application Guest Hostname:** <atl-app>
  XMI IP Address: <10.250.51.186> Netmask: <255.255.255.0> gateway: <10.250.51.1>

2.10 IDIH Blade Installation Stand-Alone

Note: Values enclosed with angle brackets <>, should be modified for your installation.

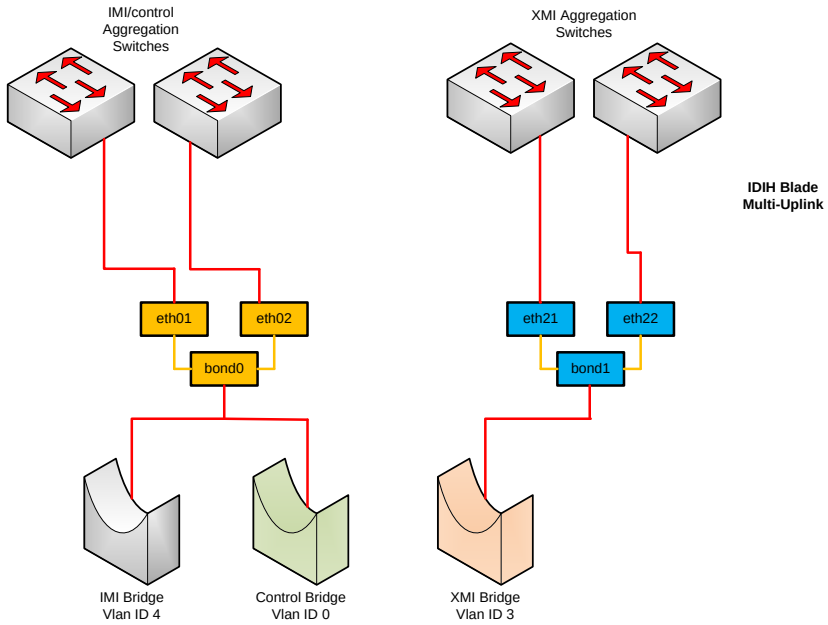
- **Enclosure Element**
  Enclosure ID: <enc1> Cabinet HW ID: <cab1> OA1 IP: <10.240.71.197> OA2 IP: <10.240.71.198>
- **Blade Element**
  Blade ID: <blade15> Enclosure HW ID: <enc1> Bay: <15F>
- **TVOE Host element**
  TVOE host ID: srvrtvoe Blade Hardware ID: <blade15> TVOE hostname: <atl-tvoe>
- **NTP servers**
  ntpserver1 IP: <10.250.32.10> ntpserver2 IP:

- **Single-Uplink (Bond0)**
  - **Config File Options:** idihBladeSingle.xml



- **TVOE XMI interface**
  Device: <bond0.3> VLAN ID: <3>
- **TVOE IMI interface**
  Device: <bond0.4> VLAN ID: <4>
- **TVOE XMI Bridge**
  Interface: <bond0.3> IP Address: <10.250.51.39> Netmask:<255.255.255.0> gateway: <10.250.51.1>
- **TVOE IMI Bridge**
  Interface: <bond0.4>
- **Oracle Guest Hostname:** <atl-ora>
  XMI IP Address: <10.250.51.184> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **Mediation Guest Hostname:** <atl-med>
  XMI IP Address: <10.250.51.185> Netmask: <255.255.255.0> gateway: <10.250.51.1>
  IMI IP Address: <192.168.10.55> Netmask: <255.255.255.0>
- **Application Guest Hostname:** <atl-app>
  Management IP Address: <10.250.51.186> Netmask: <255.255.255.0> gateway: <10.250.51.1>

- **Multi-Uplink (Bond0, Bond1)**
  - **Config File Options:** idihBladeMulti.xml



- **TVOE XMI interface**
  Device: <bond1> Bond Interfaces : <eth21,eth22>
- **TVOE IMI interface**
  Device: <bond0.4> VLAN ID: <4>
- **TVOE XMI Bridge**
  Interface: <bond1> IP Address: <10.250.51.39> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **TVOE IMI Bridge**
  Interface: <bond0.4>
- **Oracle Guest Hostname:** <atl-ora>
  XMI IP Address: <10.250.51.184> Netmask: <255.255.255.0> gateway: <10.250.51.1>
- **Mediation Guest Hostname:** <atl-med>
  XMI IP Address: <10.250.51.185> Netmask: <255.255.255.0> gateway: <10.250.51.1>
  IMI IP Address: <192.168.10.55> Netmask: <255.255.255.0>
- **Application Guest Hostname:** <atl-app>

XMI IP Address: <10.250.51.186> Netmask: <255.255.255.0> gateway: <10.250.51.1>

Chapter 3

Installation Overview

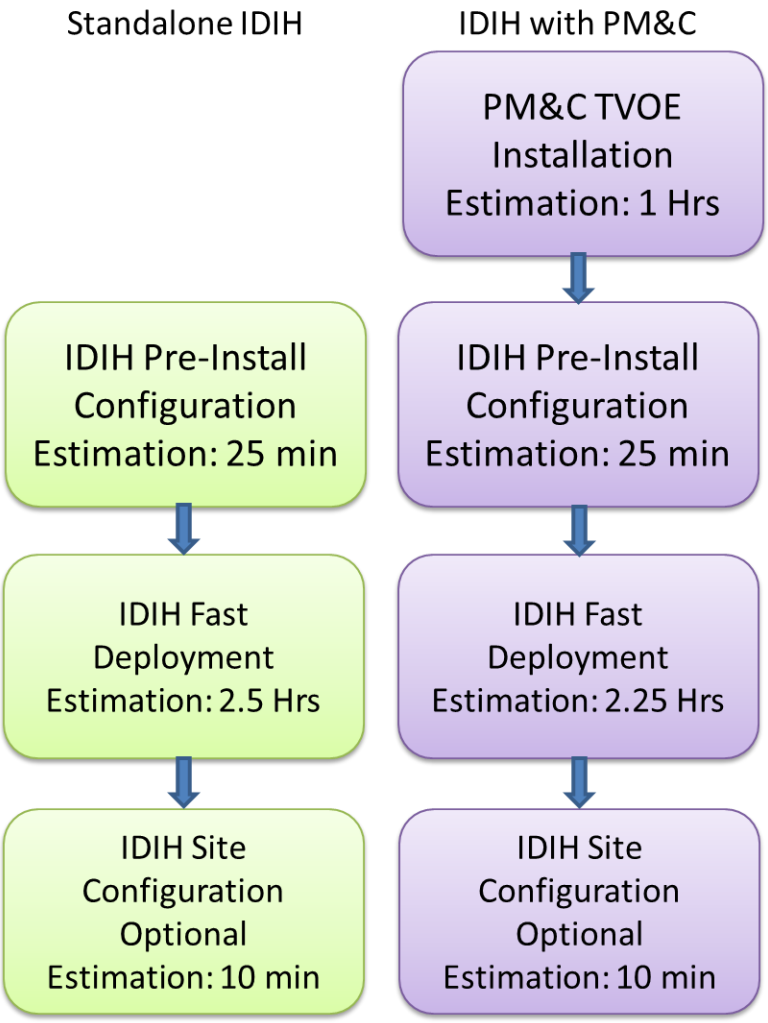
Topics:

3.1 Installation Overview

This section provides installation overview for the IDIH system. The flowcharts below depict the flow of installation for a standalone system and an IDIH system where the PM&C will co-exist on the same TVOE host. For instructions on PM&C installation refer to the DSR installation document.

Prerequisite: PM&C and DSR must be already installed and configured before performing IDIH installation.

Note: Fresh install procedure expects a clean system, you must delete the IDIH guests and remove the external drive. Please refer to Appendix C for external drive removal instructions.



Chapter 4

Installation Procedures

Topics:

4.1 Pre-install Configuration

Note: Fresh install procedure expects a clean external drive. Any logical partitions on the external drive must be removed before installation. For best performance on HP ProLiant hardware be sure to configure the HP Static High Performance Mode. Please refer to Appendix C for external drive removal instructions and the HP Static High Performance Mode.

1. **Verify the PM&C server is at PM&C 5.5 of greater. If it is not you must first upgrade the PM&C server to version 5.5 or greater.**
   a) Open a web browser and log into the PM&C server as pmacadmin.
   b) The PM&C version is listed at the top of the screen.

   Note: The Fast Deployment feature is not available in PM&C releases before version 5.5.

2. **Transfer IDIH ISO images to the PM&C Server. See Appendix B: *Adding ISO Images to the PM&C Image Repository*.**

   Warning: Each ISO must be copied and added to the PM&C repository before the next ISO is added. Due to the limited size of the temporary repository on the PM&C server. ISO's could be on USB media, follow the instructions that are appropriate in Appendix B.

   TVOE
   - TVOE-X.X.X.X.X_XX.XX.X-x86_64

   TPD
   - TPD.install-X.X.X.X.X_XX.XX.X-OracleLinux6.5-x86_64

   Application
   - apps-X.X.X_XX.XX.X-x86_64

   Mediation
   - mediation-X.X.X_XX.XX.X-x86_64

   Oracle
   - oracle-X.X.X_XX.XX.X-x86_64

3. **As admusr user on the PM&C server, copy the IDIH Fast Copy Configuration template file to the guest-dropin directory. Reference the worksheet you used to collect your configuration data and copy the appropriate FDC file to guest-dropin.**

   Note: Values enclosed with angle brackets <>, should be modified for your installation.

   ```
   # sudo cp /usr/TKLC/smac/html/TPD/*mediation*/<idih>.xml /var/TKLC/smac/guest-dropin
   ```

4. **Edit the IDIH Fast Copy Configuration template file.**

   Please review Appendix A: *Fast Deployment Configuration File Description* for the XML explanation before proceeding to the next step.

Update the following parameters in the FDC file in guest-dropin as required for a particular hardware and network configuration:

- Blade Enclosure
  - Update cabinet hardware id, enclosure id and OA ip addresses.

```
<enclosure id="enc1">
        <cabhwid>cab1</cabhwid>
        <encid>1401</encid>
        <oa1>10.240.71.197</oa1>
        <oa2>10.240.71.198</oa2>
</enclosure>
```

- Blade Server
  - Update enclosure hardware id, bay and type.

```
<blade id="blade7">
        <enchwid>enc1</enchwid>
        <bay>7F</bay>
</blade>
```

- Rack Mount Server
  - Update the Out of Band IP address, this is the address assigned to the tvoe servers ILO.

```
<rms id="mgmtsrvr">
        <rmsOOBIP>10.250.36.27</rmsOOBIP>
        <rmsname>d-ray</rmsname>
        <cabhwid>cab1</cabhwid>
        <rmsuser>root</rmsuser>
        <rmspassword>TklcRoot</rmspassword>
</rms>
```

- Configure the TVOE Host Fast Deployment ID

```
</hardware>
<tvoehost id="mgmtsrvrtvoe">
```

- Configure the TVOE Hostname

```
<serverinfo>
        <!--tvoe hostname: Update hostname-->
        <hostname>d-ray</hostname>
```

- Update ntpserver names and ip addresses

```
<!--tvoe ntpservers: Update ip address-->
        <ntpservers>
                <ntpserver>
                        <name>ntpserver1</name>
                        <ipaddress>10.250.32.10</ipaddress>
                </ntpserver>
```

```
        </ntpservers>
```

- Configure XMI Interface device and vlanid, if you don't have a tagged device then there is no need to configure vlanid.

```
<!--tvoe xmi interface: Update device and vlanid-->
<tpdinterface id="xmi">
        <device>bond0.3</device>
        <type>Vlan</type>
        <vlandata>
                <vlanid>3</vlanid>
        </vlandata>
        <onboot>yes</onboot>
        <bootproto>none</bootproto>
</tpdinterface>
```

- Configure the IMI Interface device and vlanid, if you don't have a tagged device then there is no need to configure vlanid.

```
<!--Tvoe imi interface: Update device and vlanid-->
<tpdinterface id="imi">
        <device>bond0.4</device>
        <type>Vlan</type>
        <vlandata>
                <vlanid>4</vlanid>
        </vlandata>
        <onboot>yes</onboot>
        <bootproto>none</bootproto>
</tpdinterface>
```

- Configure the TVOE XMI Bridge interface, address, and netmask.

  Note: Verify that the XMI Interface name matches the XMI device name in the XMI Interface device and vlanid.

```
<!--Tvoe xmi bridge: Update interfaces, ipaddress and netmask-->
<tpdbridge id="xmibr">
        <name>xmi</name>
        <!--Make sure this value matches the imi tpdinterface-->
        <interfaces>bond0.3</interfaces>
        <bootproto>none</bootproto>
        <address>10.240.51.39</address>
        <netmask>255.255.255.0</netmask>
        <onboot>yes</onboot>
</tpdbridge>
```

- Configure the TVOE IMI Bridge interface, address and netmask.

Note: Verify that the IMI Interface name matches the IMI device name in the IMI Interface device and vlanid.

```
<!--Tvoe imi bridge: Update interfaces, ipaddress and netmask-->
<tpdbridge id="imibr">
       <name>imi</name>
       <!--Make sure this value matches the imi tpdinterface-->
       <interfaces>bond0.4</interfaces>
       <bootproto>none</bootproto>
       <onboot>yes</onboot>
</tpdbridge>
```

- Configure the TVOE default gateway.

```
<!--Tvoe default gateway address: Update gateway-->
<tpdroute id="default">
       <type>default</type>
       <device>xmi</device>
       <gateway>10.240.30.3</gateway>
</tpdroute>
```

  - Oracle Guest
    - Configure the Oracle guest Profile. If you are configuring Gen6 hardware be sure to comment out or remove APP_GEN8 and uncomment APP_GEN6

```
<!--Application Guest Profile: Update the profile for the hardware type,
default is Gen8->
<!--profile>APP_GEN6</profile-->
<profile>APP_GEN8</profile>
```

    - Configure the Oracle guest Hostname.

```
<serverinfo>
       <!--Oracle guest hostname-->
       <hostname>mamie</hostname>
</serverinfo>
```

    - Configure the Oracle XMI address and netmask.

```
<!--Oracle Guest xmi network: Update address and netmask-->
<scriptfile id="oracleXmi">
       <filename>/usr/TKLC/plat/bin/netAdm</filename>
       <arguments>set --device=xmi --address=10.250.51.184
       --netmask=255.255.255.0 --onboot=yes --bootproto=none</arguments>
</scriptfile>
```

    - Configure Oracle guest default gateway.

```
<!--Oracle Guest xmi default route: Update gateway-->
<scriptfile id="oracleRoute">
```

```
        <filename>/usr/TKLC/plat/bin/netAdm</filename>
        <arguments>add --route=default --device=xmi
        --gateway=10.250.51.1</arguments>
</scriptfile>
```

- Mediation Guest
  - Configure the Mediation guest Hostname.

```
<serverinfo>
        <!--Mediation guest hostname-->
        <hostname>poney</hostname>
</serverinfo>
```

  - Configure the Mediation guest XMI address and netmask.

```
<!--Mediation Guest xmi network: Update address and netmask-->
        <scriptfile id="medXmi">
        <filename>/usr/TKLC/plat/bin/netAdm</filename>
        <arguments>set --device=xmi --address=10.250.51.185
        --netmask=255.255.255.0 --onboot=yes --bootproto=none</arguments>
</scriptfile>
```

  - Configure the Mediation guest Route gateway.

```
<!--Mediation Guest xmi default route: Update gateway-->
<scriptfile id="medRoute">
        <filename>/usr/TKLC/plat/bin/netAdm</filename>
        <arguments>add --route=default --device=xmi
        --gateway=10.250.51.1</arguments>
</scriptfile>
```

  - Configure the Mediation guest IMI address and netmask.

```
<!--Mediation Guest imi network: Update address and netmask-->
<scriptfile id="medImi">
        <filename>/usr/TKLC/plat/bin/netAdm</filename>
        <arguments>set --device=imi --address=192.168.10.55
        --netmask=255.255.255.0 --onboot=yes --bootproto=none</arguments>
</scriptfile>
```

- Application Guest
  - Configure the Application guest Hostname.

```
<serverinfo>
        <!--Application guest hostname: Update hostname-->
        <hostname>jesco</hostname>
</serverinfo>
```

  - Configue Application guest XMI address and netmask.

```
<!--Application Guest xmi network: Update address and netmask-->
<scriptfile id="appXmi">
       <filename>/usr/TKLC/plat/bin/netAdm</filename>
       <arguments>set --device=xmi --address=10.250.51.186
       --netmask=255.255.255.0 --onboot=yes --bootproto=none</arguments>
</scriptfile>
```

- Configure Application guest default gateway

```
<!--Application Guest xmi default route: Update gateway-->
<scriptfile id="appRoute">
       <filename>/usr/TKLC/plat/bin/netAdm</filename>
       <arguments>add --route=default --device=xmi
       --gateway=10.250.51.1</arguments>
</scriptfile>
```

5. **Validate the contents of the fast deployment configuration file on the PM&C server.**

```
[admusr@ferbpmac guest-dropin]# sudo fdconfig validate --file=<idih>.xml
Validate configuration file: "ferbrms.xml"
Configuration file validation successful.
Validation complete
```

Note: /var/TKLC/smac/guest-dropin

4.2 Fast Deployment

1. **As admusr user on the PM&C server, begin the fast deployment and configuration process.**

```
[admusr@ferbpmac guest-dropin]# sudo fdconfig config --file=<idih>.xml
run Config
Request to start a new configuration
Running ferbrms.xml configuration
Configuration file processing complete
```

2. **Monitor the progress of the installation on the PM&C GUI Task Monitoring page and from the CLI until installation is complete.**

   Note: The installation should take approximately two and half hours.

4.3 Generate Disaster Recovery FDC File

After successfully installing the system with fdconfig, you need to generate a Disaster Recovery FDC file. Simply execute the following steps to create one:

1. cd to **/var/TKLC/smac/guest-dropin** as admusr user.
2. Execute the following command to generate a disaster recovery FDC file:

```
[admusr@ferbpmac guest-dropin]# sudo /usr/TKLC/smac/html/TPD/mediation*/gen_dr_fdc_file.sh <idih>.xml
```

NOTE: The <idih>.xml file is the same fdconfig file used to fresh install the system from the PMAC server.

3. A file “DisasterRecovery_<idih>.xml” will be grenerated.
4. Save the FDC File
   It is highly recommend that you save a copy of both the fresh installation FDC file <idih>.xml and the disaster recovery FDC file “DisasterRecovery<idih>.xml” in a safe place outside of the idih system, so you can perform disaster recovery procedures later.

4.4 Post Installation Configuration

A. Configure DSR Reference Data Synchronization for IDIH

After an IDIH fresh installation, reference data synchronization is initially disabled. Reference data synchronization requires some initial configuration before it is enabled.

The Trace Ref Data Adapter application must retrieve data from web services hosted by the DSR SO web server, and this requires the DSR Site OAM virtual IP address (VIP) to be configured. The DSR SO VIP will be unique at each customer site because it is defined based on the customer's network configuration. Therefore, there is no standard default value for the DSR SO VIP.

a) Configure DSR Reference Data Synchronization for DIH.

1. Log into an IDIH app server terminal window as LINUX user **tekelec**.
2. Execute script: **apps/trda-config.sh**
3. For prompt "**Please enter DSR soam server IP address**", enter the virtual IP address of the DSR Site OAM and press Enter.
   - If the address entered is unreachable the script will exit with error "**Unable to connect to <*ip-address*>!**".
   - Entry of a reachable address causes the trace-refdata-adapter application to be enabled in the Weblogic server.
   - This is sample terminal output for a successful execution of script **apps/trda-config.sh** :

```
demo1-app:/usr/TKLC/xIH apps/trda-config.sh
dos2unix: converting file
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-
adapter.properties to UNIX format ...
Please enter DSR oam server IP address: 10.240.39.175
dos2unix: converting file /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-adapter.properties
to UNIX format ...
Buildfile: build.xml

app.disable:

common.weblogic.stop:
     [echo]
     [echo]
     [echo] ================================================================
     [echo] application: xihtra
     [echo] ================================================================
     [echo] === stop application EAR
     [java] weblogic.Deployer invoked with options:  -adminurl http://appserver:7001 -userconfigfile
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/configfile.secure -userkeyfile
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -stop
     [java] <Oct 17, 2013 11:35:32 AM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating stop operation
for application, xIH Trace Reference Data Adapter [archive: null], to configured targets.>
     [java] Task 4 initiated: [Deployer:149026]stop application xIH Trace Reference Data Adapter on nsp.
     [java] Task 4 completed: [Deployer:149026]stop application xIH Trace Reference Data Adapter on nsp.
     [java] Target state: stop completed on Server nsp
     [java]

BUILD SUCCESSFUL
Total time: 1 minute 3 seconds
Buildfile: build.xml

app.enable:

common.weblogic.start:
     [echo]
     [echo]
     [echo] ================================================================
     [echo] application: xihtra
     [echo] ================================================================
     [echo] === start application EAR
     [java] weblogic.Deployer invoked with options:  -adminurl http://appserver:7001 -userconfigfile
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/configfile.secure -userkeyfile
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -start
     [java] <Oct 17, 2013 11:36:36 AM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating start
operation for application, xIH Trace Reference Data Adapter [archive: null], to configured targets.>
     [java] Task 5 initiated: [Deployer:149026]start application xIH Trace Reference Data Adapter on nsp.
     [java] Task 5 completed: [Deployer:149026]start application xIH Trace Reference Data Adapter on nsp.
     [java] Target state: start completed on Server nsp
     [java]

BUILD SUCCESSFUL
Total time: 1 minute 3 seconds
```

4. Monitor log file **`/var/TKLC/xIH/log/apps/weblogic/apps/application.log`** for log entries containing text "**Trace Reference Data Adapter**".

B. Setting up the SSO Domain.

Note: *Oracle highly recommends implementing SSO in combination with IDIH. SSO provides seamless integration of iDIH feature into DSR which is part of the original design intent. Only sites that do not support DNS should rely on this alternate authentication method*

a) Confirm that DNS has been configured in the DSR OAM.

1. Log into the DSR ACTIVE NETWORK OAM&P as user **guiadmin.**
2. Access menu **Administration->Remote Servers->DNS Configuration** to display the web

page.

3. In the System Domain section of the page, Confirm that a value has been entered for field **Domain Name**.
4. In the External DNS Name Servers section of the page, confirm that field **Name Server 1** has a value.
5. In the Domain Search Order section of the page, confirm that field **Search Domain 1** has a value.
6. If any previously mentioned field is not configured, consult the network administrator for proper configuration values before proceeding with steps in this section.
7. Select the Cancel button.

b) Establish the SSO Local Zone in the DSR OAM.

1. Log into the DSR ACTIVE NETWORK OAM&P as user **guiadmin**.
2. Access menu **Administration->Access Control->Certificate Management**.
3. Select button **Establish SSO Zone**.
4. In the **Establish Single Sign-On Authentication Zone** page, enter a value for field **Zone Name**. Example: **dsr**.
5. Select the **Ok** button. Information for the new Certificate of type **SSO** Local is displayed.
6. Select the **Report** button. The Certificate Report is displayed. Select and copy the encoded certificate text to the clipboard for future access. Example:

```
-----BEGIN CERTIFICATE-----
MIIEPzCCAyegAwIBAgIBADANBgkqhkiG9w0BAQUFADCBuTELMAkGA1UEBhMCVVMx
FzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRQwEgYDVQQHDAtNb3JyaXN2aWxsZTEQ
MA4GA1UECgwHVGVrZWxlYzERMA8GA1UECwwIQXBwV29ya3MxMjAwBgNVBAMMKWRz
ci9kb21haW49bGFicy5uYy50ZWtlbGVjLmNvbS90eXBlPUFXU1NPMSIwIAYJKoZI
hvcNAQkBFhNzdXBwb3J0QHRla2VsZWMuY29tMB4XDTEzMDgyNjE3NDM1NVoXDTE0
MDgyNjE3NDM1NVowgbkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIDA5Ob3J0aCBDYXJv
bGluYTEUMBIGA1UEBwwLTW9ycmlzdmlsbGUxEDAOBgNVBAoMB1Rla2VsZWMxETAP
BgNVBAsMCEFwcFdvcmtzMTIwMAYDVQQDDClkc3IvZG9tYWluPWxhYnMubmMudGVr
ZWxlYy5jb20vdHlwZT1BV1NTTzEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEB0ZWtl
bGVjLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANA7uB1JTv1x
hLKz7Fj7rcH0pqzNUKThUStQkAplOUuOYjMHz5gCBdRqu4LnHRtJ+fIHxAzIoksp
V1C0Ucsl4V+ptAySbQH4cv5swrzAZp2ntzdqqNs3EPFeRwy80Ok9mV4glM1c5ozq
V3EyjE37Bt0kBH1qhiqLhsepvqflGVboZok4zZoCFl4VKfYzCg4wIjhhSTx74o8G
cRG6mNt14xDBNOUaXvngnyrEjvb4ckwbH43hl+0zbBptFV+aRwPrcFpuZ3zaolaf
P7vOK5S8gSgYblnA/DZ2WrXmShxUp8bpH//rH6HS4TvVPSswUnnfyruK48uTogLP
E+v9Mi6UY8ECAwEAAaNQME4wHQYDVR0OBBYEFI9KwcaTlMyoZmNgC1snxjHsAQXM
MB8GA1UdIwQYMBaAFI9KwcaTlMyoZmNgC1snxjHsAQXMMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQEFBQADggEBAI96pB+IvJ8xN8agrhE4lVCqL0v2AlqYKRVnASGW
XUYRMkaBEX/soqCHEfj3tS79XOZVajgCcsga0Q/eMw8+1srqNpPJ/u5IwOxnmsE1
nph11+nV9ekUNtvKh53iVjHKYMtoCMEblgEc9O8/rUtxoVz9qIf2EEkSWlazx7UR
iAaB04C0lEXjReHPy0TIqPJzIIsOiAMAza/FdLLEukIqBk3Qg/jkCDe4uCC3zzTu
TGagLMW4oDYxhYuFs5B3m51rBI8arDx4j2TfJVu6Q1pHs0TQu+vRooH1YXxJoJc6
94UUa/UsuamVifGktkcOMenYQbgHvmUXQ/Hic+4adFkA6uE=
       -----END CERTIFICATE-----
```

c) Configure the SSO Domain in the IDIH App Server

1. Log into the IDIH App Server web interface as default user **idihadmin**.
2. Select the OAM portal icon to launch the OAM web application.
3. In the IDIH OAM application, select menu **System->Single Sign On**.
4. In the **System: Single Sign On** page, select the **SSO Parameters** tab.
5. In the **SSO Domain** data entry form, select the **Edit Value** icon button.

6. Enter a value for field **Domain Name**. This should be the same domain name assigned in the DSR OAM&P DNS configuration.
7. Select the **Save** icon button.

d) IDIH App Server: Configure an SSO Remote Zone for the DSR NOAM

1. Log into the IDIH App Server web interface as default user **idihadmin**.
2. Select the OAM portal icon to launch the OAM web application.
3. In the IDIH OAM application, select menu **System->Single Sign On**.
4. In the **System: Single Sign On** page, select the **SSO Zones** tab.
5. In the **SSO Remote Zones** data entry form, select the **Add** icon button.
6. Enter a value for field **Remote Name**. This should be the name for the SSO Local Zone that was configured in the DSR Network OAM&P.
7. In field **X.509 Certificate**, paste the encoded certificate text from the clipboard that was previously copied from the DSR Network OAM&P.
8. Select the **Save** icon button.
9. Select the **Refresh** icon button to display data saved for the Remote Zone.

C. Configure IDIH in the DSR

There are two configuration actions that need to take place on the DSR to complete the iDIH integration. The first action, comAgent configuration, takes place on the NOAMP. The second, iDIH configuration, takes place on the SOAM.

a) DSR NOAM: Configure the IDIH Mediation Server as a Communication Agent Remote Server

1. Open a new web browser window/tab and login to the DSR System NOAM.
2. Select menu **"Communication Agent->Configuration->Remote Servers"**
3. Add the IDIH Mediation server:
   - Use the *IMI* host IP address of the IDIH Mediation server in the *Remote Server IP Address* field
   - *Remote Server Mode* field must be *Server*
4. Select menu **"Diameter->Troubleshooting with DIH->Configuration->Options"**.
   - Select the DIH IP Address and verify the field has been updated pre the previous step.

b) DSR SOAM: Configure the ProTrace Launch URL

1. Open a new web browser window/tab and login to the DSR System SOAM.
2. Select menu **"Diameter->Troubleshooting with DIH->Configuration->Options"**.
3. In field **"DIH Visualization address"**, enter the fully qualified IDIH host name. This host name includes the domain as a suffix. The domain is the same as the domain configured in the DSR DNS Configuration.
4. Click the Apply button.

D. 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 Application server.

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

   # sudo 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

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

1. Connect to the Weblogic GUI interface.
2. Log in as weblogic on the WebLogic Console. (http://<IDIH Web Server>/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=25
   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 admusr on the app server and run:

   # sudo service nspservice restart

F. 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 application server.

1. Open a terminal window and log in as admusr 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 admusr, run:

   # sudo 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.

G. Change Network Interface **(Optional)**

Initially the default network interface used to transport TTRs from DSR to DIH uses the internal imi network, however, this can be changed if required. It should be noted that changing this interface could degrade performance of TTR transmission.

A script is provided to manage the settings so that the operator doesn't need to know the details required to apply the settings. There are two settings 'interface.name ' and 'interface.enabled'. When interface.enabled=True then communications over the 'interface.name =*value*', where *value* is the name of the network interface as defined on the platform, is the only specified interface that is used for communications. When 'interface.enabled=False' then communications over the named interface is not inforced, that is,

all interfaces configured on the platform are allowed to be used for communications.
For example, if it is required to use the xmi interface for communication instead of the default internal imi interface, then the operator would supply 'xmi' when prompted for the interface name and 'True' when prompted if interface filtering should be applied.

The settings by default are as follows (only use interface imi):

a. interface.name=imi
b. interface.enabled=True

To change the network interface perform the following steps.

1. Logon to the mediation server as user admusr
2. Switch user to root with command: su –
3. Switch user to tekelec with command: su – tekelec
4. Execute chgIntf script with command: chgIntf.sh
5. Answer script questions.

Example for changing interface to xmi:

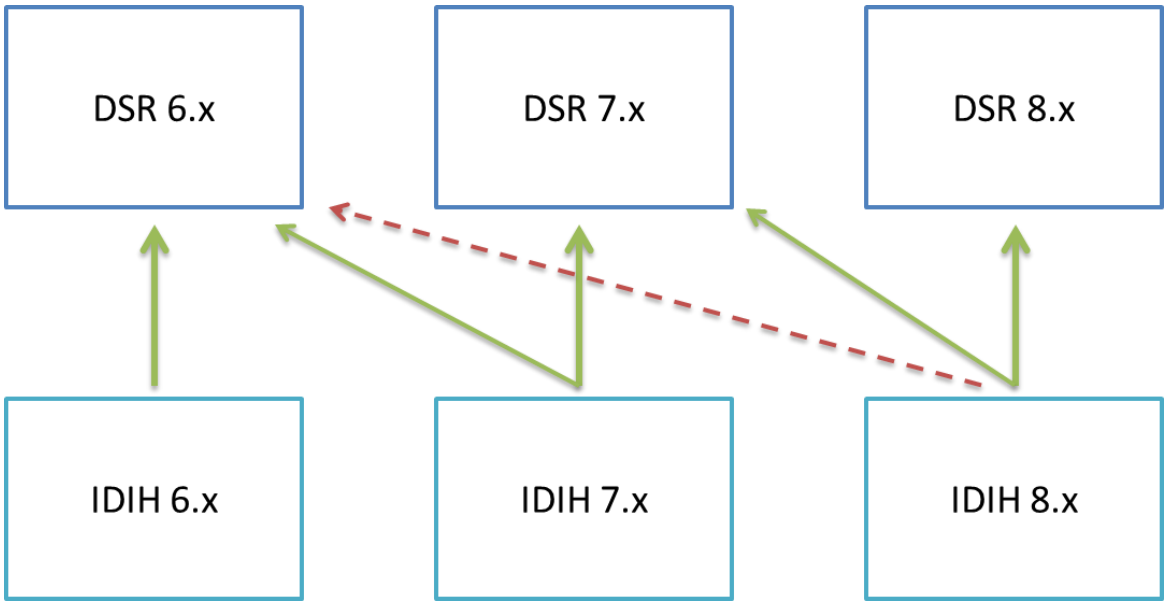
```
chgIntf.sh

This script is used to change the interface name (default = imi) used for mediation
communications and whether to enable network interface filtering or not.  Please answer the
following questions or enter CTLR-C to exit out of the script.

Current setting are: interface.name=imi interface.enabled=True

Enter new network interface name, return to keep current [imi]: xmi
Do you want to enable network interface filtering [True|False], return to keep current [True]:
Updating configuration properties file with 'interface.name=xmi' and 'interface.enable=True',
and restarting mediation configuration bundle...
```

Chapter 5

Upgrade Procedures

Topics:

5.1 Upgrade Precedence



IDIH upgrades Must be performed before the DSR upgrade . Upgrading DSR before IDIH may render IDIH non-operational till it is upgraded

IDIH will follow DSR release numbering scheme. First release of IDIH versioned 6.0 will be compatible with DSR 6.0 release. Any subsequent IDIH releases/upgrades will be always compatible with 2 Major DSR Releases and their point releases:

1.) Current Major DSR release (and its point releases) whose Major Version matches the IDIH Major version
2.) Previous (Last) DSR released version(Major and Point)

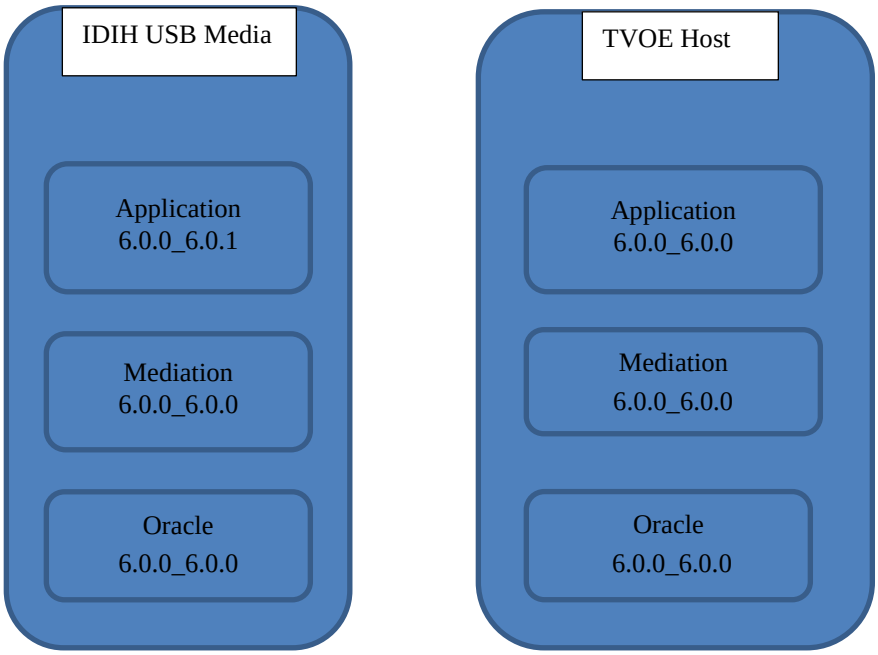
Please see above the diagram that illustrates the release compatibility. IDIH 7.x release will be compatible with DSR 7.x releases and backward compatible with DSR 6.x releases. IDIH 8.x release will be compatible with DSR 8.x releases and backward compatible with DSR 7.x releases and so on. However an IDIH 8.x will not be backwardly compatible to a DSR 6.x.

5.2 Upgrade

Although, IDIH upgrade uses the same media for upgrade as is used for install, IDIH differs on a few major points:

- It does not use `fdconfig`. Instead the PM&C GUI is used to upgrade the IDIH guests individually.
- Upgrade may only update a subset of the guests that are part of IDIH.

The last point is very important, in that the USB media or image which distributes the IDIH ISO's will always contain all the component ISO's, however only some component releases may be newer than the releases installed on the guests. The following diagram shows an example of this:



In the diagram above the only component that needs upgrading is the Application server.

The high level process of the upgrade is as follows:

1 Determine which guests need upgrading verify via PM&C GUI.
2 Import the ISO's for those guests into PM&C
3 Shutdown guests that need to be shutdown.
4 Run the upgrade of each of these guests one at a time using the PM&C `Upgrade` option for each guest to be upgraded.
5 Once all the upgrades are complete, accept each upgrade using the PM&C `Accept Upgrade` option for each guest that was upgraded.

5.3 Upgrade Failures

In the event that an upgrade failure occurs, the guest being upgraded will backoutof it's upgrade automatically. Any other guests that have been upgraded need to be manually backed out. In the event that all upgrades succeeded but for some reason it is wished that the upgrade of IDIH be backed out then each guest upgraded will need to have its upgrade rejected. Rejections are done via the PM&C GUI and is documented in section 5.11, Failed Upgrade Procedures.

5.4 Upgrade Order

The IDIH guests should be upgraded in the following order:

- Oracle Server
- Mediation Server
- Application Server

If any component is not being upgraded the order stays the same but the component that is not being upgraded is skipped. So for instance if only the Application and Mediation guests are being upgraded, then the order would be:

- Mediation
- Application

If it was only the Oracle and Mediation guests being upgraded, it would be:

- Oracle
- Mediation

5.5 Shutting Down Guests During an Upgrade

It is necessary during an upgrade to shutdown the specific Guests, and bring them back up one at a time in preparation to be upgraded.

The following chart shows the systems to be upgrade to systems to be shutdown relationship:

Guest to Be Upgraded	Guests to be Shutdown
Oracle	Mediation, Application
Mediation	Application
Application	None

5.6 Upgrade Procedure

This procedure is divided up by each guest that could be upgraded. It is meant to be started at the point of the highest precedent upgrade (see section 5.3). For instance if you were upgrading all three guests then you would start at the Oracle section, but if you were only upgrading the Application guest then you would start at the Application section. The upgrade procedure can be followed from the start point to the end no matter which guests are being upgraded.

In all cases you need to import the media into the repository:

1. **Transfer IDIH ISO images to the PM&C Server. Be sure to only copy in the ones that need to be upgraded as identified from section 5.1. See Appendix B for instructions on how to do this: *Adding ISO Images to the PM&C Image Repository*.**

   Warning: Each ISO must be copied and added to the PM&C repository before the next ISO is added, due to the limited size of the temporary repository on the PM&C server. ISO's could be on USB media, follow the instructions that are appropriate in Appendix B.

   - Application
     - apps-x.x.x_x.x.x-x86_64
   - Mediation
     - mediation-x.x.x_x.x.x-x86_64
   - Oracle
     - oracle-x.x.x_x.x.x-x86_64

Now that you have done this go to the appropriate procedure to begin the upgrade.

5.7 Oracle Upgrade Procedure

If the set of guests to be upgraded includes Oracle, then you should start with this procedure.

1. **Shutdown the application guest by logging in as admusr and running "sudo init 0"**
2. **Shutdown the mediation guest by logging in as admusr and running "sudo init 0"**
3. **Start the upgrade of the oracle guest via the PM&C GUI.**

   To do this, go to the PM&C " VM Management" Menu, select the oracle guest, and finally click on the "Upgrade" button.

4. **Monitor the upgrade till it finishes using the PM&C GUI.**

   To do this go to the Task Monitoring menu and wait till your upgrade task finishes. When it finishes your status will either say "Success" or "Failed…".

5. **If the upgrade task failed go to Section 5.11 (Failed Upgrade Procedures. Otherwise go to the next step.**
6. **If the oracle guest was upgraded, then accept the upgrade via the PM&C GUI.**
   To do this , go to the PM&C "VM Management" Menu, select the oracle guest, and finally click on the "Accept" button.
7. **Now perform a system health check on the guest. If there are errors stop this procedure and call customer service.**

To do this login in to the guest as the admusr user and run the analyze script.
$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i

8. **If the oracle guest was upgraded, then accept the upgrade via the PM&C GUI.**

   To do this , go to the PM&C "VM Management" Menu, select the oracle guest, and finally click on the "Accept" button.

5.8 Mediation Upgrade Procedure

If the set of guests to be upgraded includes Mediation but does not include Oracle, then you should start here.

1. **If the mediation guest was shutdown bring it up using the PM&C GUI:**

   To do this, go to the PM&C "VM Management" Menu, select the mediation guest, and finally under the Current Power State change the drop down menu to "On" and press the "Change To" button. This will as if you are sure you want to do this. Select "OK".

2. **Monitor the progress of the rebooting system from the PM&C GUI:**

   To do this, go to the PM&C " VM Management" Menu, select the mediation guest and check the "Upgrade" button until it is available.

   (NOTE: You may need try this procedure few more times until the "Upgrade" button is available)

3. **If you do not need to upgrade the mediation guest go to section 6.4, Application Upgrade Procedure.**

4. **Start the upgrade of the mediation guest via the PM&C GUI.**

   To do this, go to the PM&C " VM Management" Menu, select the mediation guest, and finally click on the "Upgrade" button.

5. **Monitor the upgrade till it finishes using the PM&C GUI.**

   To do this go to the Task Monitoring menu and wait till your upgrade task finishes. When it finishes your status will either say "Success" or "Failed…".

6. **If the upgrade task failed go to Section 5.10 (Failed Upgrade Procedures). Otherwise go to the next procedure.**

7. **Now perform a system health check on the guest. If there are errors stop this procedure and call customer service.**

   To do this login in to the guest as the admusr user and run the analyze script.
   $ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i

5.9 Application Upgrade Procedure

If the set of guests to be upgraded includes Application but does not include Oracle or Mediation, then you should start here.

1. **If the application guest was shutdown bring it up using the PM&C GUI:**

To do this, go to the PM&C "VM Management" Menu, select the application guest, and finally under the Current Power State change the drop down menu to "On" and press the "Change To" button. This will as if you are sure you want to do this. Select "OK".

2. **Monitor the progress of the rebooting system from the PM&C GUI:**

   To do this, go to the PM&C " VM Management" Menu, select the application guest and check the "Upgrade" button until it is available.

   (NOTE: You may need try this procedure few more times until the "Upgrade" button is available)

3. **Start the upgrade of the application guest via the PM&C GUI.**

   To do this, click on the "Upgrade" button.

4. **Monitor the upgrade till it finishes using the PM&C GUI.**

   To do this go to the Task Monitoring menu and wait till your upgrade task finishes. When it finishes your status will either say "Success" or "Failed…".

5. **If the upgrade task failed go to Section 5.10 (Failed Upgrade Procedures). Otherwise go to the next procedure.**

6. **Now perform a system health check on the guest. If there are errors, stop this procedure and call customer service.**

   To do this login in to the guest as the admusr user and run the analyze script.
   $ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i

5.10 Accept Guest Upgrades Procedure

Warning: Once accept is performed you cannot backout.

9. **If the mediation guest was upgraded, then accept the upgrade via the PM&C GUI.**

   To do this , go to the PM&C "VM Management" Menu, select the mediation guest, and finally click on the "Accept" button.

10. **If the application guest was upgraded, then accept the upgrade via the PM&C GUI.**

    To do this , go to the PM&C "VM Management" Menu, select the application guest, and finally click on the "Accept" button.

5.11 Failed Upgrade Procedure

In the event that your upgrade fails customer support should be called.

Oracle guest backout is not supported. If it is an oracle database upgrade failure, clean installation the whole IDIH system is required because backout is not supported.

For mediation and applicaton guest, when the upgrade fails it will either fail at a point that it will need to backout, or it will fail before that. If it fails past the point it needs to backout, it will do so automatically. A customer support person should then look at the system to determine what was the root cause.

If you had already upgraded other systems you will need to reject each of their upgrades so that the entire IDIH system will be at a consistent release level that was tested together. The order of upgrade should be the order of rejects. It may be that one want to reject the upgrade after a successful upgrade. This procedure will help for that also.

5.12 Reject Oracle Upgrade

Oracle upgrade does NOT support Reject(rollback). Oracle Enterprise database is its own product and controls its upgrade independently from TPD upgrade mechanism. Once upgraded, always accept its upgrade.

5.13 Reject Mediation Upgrade

1. **Reject the mediation guest upgrade via the PM&C GUI:**

   To do this, go to the PM&C "VM Management" Menu, select the mediation guest, and finally select "Reject Upgrade".

2. **Monitor the backout via the PM&C GUI**

   To do this, go to the PM&C "Task Monitoring" screen and watch until your reject task becomes complete.

5.14 Reject Application Upgrade

1. **Reject the application guest upgrade via the PM&C GUI:**

   To do this, go to the PM&C "VM Management" Menu, select the application guest, and finally select "Reject Upgrade".

2. **Monitor the backout via the PM&C GUI**

   To do this, go to the PM&C "Task Monitoring" screen and watch until your reject task becomes complete.

Appendix A

Fast Deployment Configuration File Description

Topics:

Fast Deployment Configuration File Description

An XML configuration file is the primary source of automated deployment and configuration information for the feature. The configuration defines one or more infrastructures that represents a set of hardware, software and TVOE hosts associated with a PM&C. The file also defines one or more application servers that are to be deployed to a specified infrastructure.

The sections to be modified are identified below with a brief description

Note: Any sub-element that is not described should not be modified.

More information on the FDC Fast deployment configuration file can be found in the *TR007249 Fast Deployment and Configuration Tool Technical Reference*.

A.1 Software Element

The optional `software` element contains one or more `image` elements representing deployable ISO images. Each image element has a required id attribute used to uniquely reference that image in the configuration file. The only element that should be modified is the name.

Name defines the iso version of TVOE, application, mediation, oracle or TPD image. Make sure that the versions match the version of software that you intend to install. If they do not then modify them as needed.

A.2 Enclosure Element

The enclosure element specifies the enclosure for a set of blade servers.

`cabhwid` refers to the cabinet identification used at each site.

`encid` refers to the enclosure identification used at each site.

`oa1` refers to the IP Address for the first OA within an enclosure.

`oa2` refers to the IP Address for the second OA within an enclosure.

A.3 Blade Element

The `blade` element specifies the blade within an enclosure that you intend to install an IDIH system on.

Use the `enchwid,` that has been specified within the PM&C that you intend to IPM.

`bay` is the bay location of the blade you intend to IPM.

`type` is the hardware type whether it be a Gen 6 or Gen 8 blade.

A.4 RMS Element

The `rms` element specifies a rack-mount server in the infrastrucure and provisions it in PM&C if not already present. The `rmsOOBIP`, `rmsname` and `cabhwid` elements should be modified.

The `rmsOOBIP` sub-element is the only required sub-element, and it specifies the IP address of the RMS iLO.

The `rmsname` sub-element specifies the name of the RMS when provisioned in PM&C. The `cabhwid` sub-element specifies the ID of the cabinet.

A.5 TVOE Software Element

The TVOE software stanza should not be added to an IDIH system where the IDIH guest is co-located with a PM&C guest.

Note: Do not IPM the TVOE host when the IDIH guest and PM&C guest are on the same TVOE host.

A.6 TVOE Serverinfo Element

A `serverinfo` element specifies configuration information for TVOE hosts, guest and native application servers. The only subelements that should be changed are the TVOE hostname and TVOE ntpserver ipaddress.

The `hostname` subelement sets the hostname for the TVOE host.

The `ntpservers` subelement sets NTP servers for the system. It may contain up to five `ntpserver` subelements. Each `ntpserver` element contains `name` and `ipaddress` subelements which are the host name and IP addresss of the NTP servers.

A.7 TVOE tpdinterface Sub-Element

This `tpdinterface` subelement specifies the TVOE interface configuration. The only subelements that should be modified are the `device`, `type`, `vlandata` and `vlandid` elements.

`device` contains the name of the TVOE interface device.

`type` can either be `Vlan` or `Bonding`.

`vlandata` contains a `vlanid` sub-element with the ID of the vlan.

A.8 TVOE tpdbridge Sub-Element

Each `tpdbridge` subelement specifies the TVOE bridge configuration. The subelements that should be modified are `interfaces`, `address` and `netmask`.

`interfaces` which defines the interfaces in the TVOE host bridge.

`address` defines the IP address of the TVOE host bridge.

`netmask` defines the network mask for the TVOE host bridge.

A.9 TVOE tpdroute Sub-Element

This `tpdroute` subelement specifies the TVOE route configuration. The only subelement that should be modified is the `gateway`.

`gateway` specifies the gateway for the XMI route used by the TVOE host.

A.10 Oracle Guest Scripts Element Network

The scripts element defines files that will be executed as part of the IPM process. Currently network configuration of the tvoe guest is not directly supported by the Fast Deployment. So we must call the netAdm script with Arguments. The only Arguments that should be modified are the `address`, `netmask` and `gateway`.

`address` defines the IP XMI address of the oracle guest.

`netmask` defines the oracle guest XMI netmask.

`gateway` defines the XMI default route used by the oracle guest

A.11 Mediation Guest Scripts Element Network

The scripts element defines files that will be executed as part of the IPM process. Currently network configuration of the tvoe guest is not directly supported by the Fast Deployment. So we must call the netAdm script with Arguments. The only Arguments that should be modified are the `address`, `netmask` and `gateway`.

`address` defines the IP XMI and IMI address of the mediation guest.

`netmask` defines the mediation guest XMI and IMI netmask.

`gateway` defines the XMI default route used by the mediation guest

A.12 Application Guest Scripts Element Network

The scripts element defines files that will be executed as part of the IPM process. Currently network configuration of the tvoe guest is not directly supported by the Fast Deployment. So we must call the netAdm script with Arguments. The only Arguments that should be modified are the `address`, `netmask` and `gateway`.

`address` defines the IP XMI address of the application guest.

`netmask` defines the application guest XMI netmask.

`gateway` defines the XMI default route used by the application guest

NOTE: **Prior** to 6.0.2, in the tvoehost/predeploy/scriptfile/configExt stanza, the script used to configure the external disk is H/W dependent:

- HP H/W uses the external.pl script.
- SUN H/W uses external.sh script.

If you are using 6.0.2, then use external.sh for both HP and Sun H/W.

```
<fdc>
       <infrastructures>
       <infrastructure name="PMAC">
              <!--Software Elements-->
              <software>
                  <image id="tvoe">
                     <name>872-2525-101-2.5.0_82.12.1-TVOE-x86_64</name>
                  </image>
                  <image id="app">
                     <name>872-2427-102-6.0.0_6.0.0-apps-x86_64</name>
                  </image>
                  <image id="med">
                     <name>872-2427-101-6.0.0_6.0.0-mediation-x86_64</name>
                  </image>
                  <image id="ora">
                     <name>872-2440-104-6.0.0_6.0.0-oracle-x86_64</name>
                  </image>
                  <image id="tpd">
                     <name>TPD.install-6.5.0_82.15.0-CentOS6.4-x86_64</name>
                  </image>
              </software>
              <hardware>
              <cabinet id="cab1">
                     <cabid>1</cabid>
              </cabinet>

              <!--Enclosure Element: Update cabhwid, endid and oa ip's-->
              <enclosure id="enc1">
                      <cabhwid>cab1</cabhwid>
                      <encid>1401</encid>
                      <oa1>10.240.71.197</oa1>
                      <oa2>10.240.71.198</oa2>
               </enclosure>

               <!--Blade Element: Update enchwid, bay and type-->
               <blade id="blade7">
                       <enchwid>enc1</enchwid>
                       <bay>7F</bay>
                       <type>ProLiant BL460c G6</type>
               </blade>
```

```
<!--Rack Mount Server Element: update rmsOOBIP with ILO IP-->
<rms id="mgmtsrvr">
      <rmsOOBIP>10.250.36.27</rmsOOBIP>
      <rmsname>d-ray</rmsname>
      <cabhwid>cab1</cabhwid>
      <rmsuser>root</rmsuser>
      <rmspassword>TklcRoot</rmspassword>
      <type>ProLiant DL380 G8</type>
</rms>
</hardware>
<tvoehost id="mgmtsrvrtvoe">

      <!--TVOE Hardware Element: Update the name of the tvoe device-->
      <!--In this example we are configuring a rms server-->
      <hardware>
            <rmshwid>mgmtsrvr</rmshwid>
            <!--bladehwid>blade7</bladehwid-->
      </hardware>

      <!--TVOE Software Element-->
      <!--Do Not Use this element when the PM&C host co-exist with IDIH-->
      <!--software>
        <baseimage>tvoe</baseimage>
      </software-->
      <serverinfo>

        <!--tvoe hostname: Update hostname-->
        <hostname>d-ray</hostname>

        <!--tvoe ntpservers: Update ip address-->
        <ntpservers>
           <ntpserver>
              <name>ntpserver1</name>
              <ipaddress>10.250.32.10</ipaddress>
           </ntpserver>
        </ntpservers>
      </serverinfo>
      <tpdnetworking>
        <tpdinterfaces>

          <!--tvoe xmi interface: Update device and vlanid-->
          <tpdinterface id="xmi">
            <device>bond0.3</device>
            <type>Vlan</type>
            <vlandata>
              <vlanid>3</vlanid>
            </vlandata>
            <onboot>yes</onboot>
            <bootproto>none</bootproto>
          </tpdinterface>

          <!--Tvoe imi interface: Update device and vlanid-->
          <tpdinterface id="imi">
            <device>bond0.4</device>
            <type>Vlan</type>
            <vlandata>
              <vlanid>4</vlanid>
            </vlandata>
            <onboot>yes</onboot>
            <bootproto>none</bootproto>
          </tpdinterface>
        </tpdinterfaces>
        <tpdbridges>

          <!--Tvoe xmi bridge: Update interfaces, ipaddress and netmask-->
          <tpdbridge id="xmibr">
            <name>xmi</name>
            <!--Make sure this value matches the imi tpdinterface-->
            <interfaces>bond0.3</interfaces>
            <bootproto>none</bootproto>
            <address>10.240.51.39</address>
            <netmask>255.255.255.0</netmask>
            <onboot>yes</onboot>
          </tpdbridge>

          <!--Tvoe imi bridge: Update interfaces, ipaddress and netmask-->
          <tpdbridge id="imibr">
            <name>imi</name>
            <!--Make sure this value matches the imi tpdinterface-->
            <interfaces>bond0.4</interfaces>
            <bootproto>none</bootproto>
            <onboot>yes</onboot>
```

```
                        </tpdbridge>
                        <tpdbridge id="intbr">
                          <name>int</name>
                          <bootproto>none</bootproto>
                          <onboot>yes</onboot>
                        </tpdbridge>
                      </tpdbridges>
                      <tpdroutes>

                         <!--Tvoe default gateway address: Update gateway-->
                         <tpdroute id="default">
                            <type>default</type>
                            <device>xmi</device>
                            <gateway>10.240.30.3</gateway>
                         </tpdroute>
                      </tpdroutes>
                    </tpdnetworking>
                    <scripts>
                    <predeploy>

                      <!--configExt configures external disk-->
                      <scriptfile id="configExt">
                        <image>med</image>
                        <imagefile>external.sh</imagefile>
                        <filename>/root/external.sh</filename>
                      </scriptfile>
                    </predeploy>
                    </scripts>
              </tvoehost>
            </infrastructure>
      </infrastructures>
      <servers>

            <!--Oracle Guest Configuration-->
            <tvoeguest id="Oracle">
                  <infrastructure>PMAC</infrastructure>
                  <tvoehost>mgmtsrvrtvoe</tvoehost>

                  <!--Oracle Guest Profile: Update if hardware is Gen6 default is Gen8-->
                  <!--profile>ORA_GEN6</profile-->
                  <profile>ORA_GEN8</profile>
                  <name>oracle</name>
                  <software>
                      <baseimage>tpd</baseimage>
                      <appimage>ora</appimage>
                  </software>
                  <serverinfo>

                      <!--Oracle guest hostname-->
                      <hostname>mamie</hostname>
                  </serverinfo>
                  <scripts>
                      <presrvapp>
                         <scriptfile id="oracleInt">
                              <filename>/usr/TKLC/plat/bin/netAdm</filename>
                              <arguments>set --device=int --address=10.254.254.2 --netmask=255.255.255.224 --
onboot=yes --bootproto=none</arguments>
                          </scriptfile>

                          <!--Oracle Guest xmi network: Update address and netmask-->
                         <scriptfile id="oracleXmi">
                              <filename>/usr/TKLC/plat/bin/netAdm</filename>
                              <arguments>set --device=xmi --address=10.250.51.184 --netmask=255.255.255.0 --
onboot=yes --bootproto=none</arguments>
                          </scriptfile>

                          <!--Oracle Guest xmi default route: Update gateway-->
                          <scriptfile id="oracleRoute">
                              <filename>/usr/TKLC/plat/bin/netAdm</filename>
                              <arguments>add --route=default --device=xmi --gateway=10.250.51.1</arguments>
                          </scriptfile>
                      </presrvapp>
                      <postsrvapp>

                         <!--Oracle Post Server Application Configuration Script-->
                         <scriptfile id="oracleConfig">
                              <filename>/opt/xIH/oracle/configureOracle.sh</filename>
                              <timeout>2700</timeout>
                          </scriptfile>
                      </postsrvapp>
                  </scripts>
            </tvoeguest>
```

```
            <!--Mediation Guest Configuration-->
            <tvoeguest id="Mediation">
                  <infrastructure>PMAC</infrastructure>
                  <tvoehost>mgmtsrvrtvoe</tvoehost>

                  <!--Mediation Guest Profile: Update if hardware is Gen6 default is Gen8-->
                  <!--profile>MED_GEN6</profile-->
                  <profile>MED_GEN8</profile>
                  <name>mediation</name>
                  <software>
                      <baseimage>tpd</baseimage>
                      <appimage>med</appimage>
                  </software>

                  <!--Mediation guest hostname-->
                  <serverinfo>
                      <hostname>poney</hostname>
                  </serverinfo>
                  <scripts>
                      <presrvapp>
                         <scriptfile id="medInt">
                              <filename>/usr/TKLC/plat/bin/netAdm</filename>
                              <arguments>set --device=int --address=10.254.254.3 --netmask=255.255.255.224 --
onboot=yes --bootproto=none</arguments>
                          </scriptfile>

                          <!--Mediation Guest xmi network: Update address and netmask-->
                         <scriptfile id="medXmi">
                              <filename>/usr/TKLC/plat/bin/netAdm</filename>
                              <arguments>set --device=xmi --address=10.250.51.185 --netmask=255.255.255.0 --
onboot=yes --bootproto=none</arguments>
                          </scriptfile>

                          <!--Mediation Guest xmi default route: Update gateway-->
                          <scriptfile id="medRoute">
                             <filename>/usr/TKLC/plat/bin/netAdm</filename>
                             <arguments>add --route=default --device=xmi --gateway=10.250.51.1</arguments>
                          </scriptfile>

                          <!--Mediation Guest imi network: Update address and netmask-->
                          <scriptfile id="medImi">
                              <filename>/usr/TKLC/plat/bin/netAdm</filename>
                              <arguments>set --device=imi --address=192.168.10.55 --netmask=255.255.255.0 --
onboot=yes --bootproto=none</arguments>
                          </scriptfile>
                      </presrvapp>

                      <!--Mediation Post Deploy Database Configuration Script-->
                      <postdeploy>
                         <scriptfile id="medConfig">
                              <filename>/opt/xIH/mediation/xdrDbInstall/install.sh</filename>
                          </scriptfile>
                      </postdeploy>
                  </scripts>
            </tvoeguest>

            <!--Application Guest Configuration-->
            <tvoeguest id="Application">
                  <infrastructure>PMAC</infrastructure>
                  <tvoehost>mgmtsrvrtvoe</tvoehost>

                  <!--Application Guest Profile: Update if hardware is Gen6 default is Gen8-->
                  <!--profile>APP_GEN6</profile-->
                  <profile>APP_GEN8</profile>
                  <profile>application</profile>
                  <name>application</name>
                  <software>
                      <baseimage>tpd</baseimage>
                      <appimage>app</appimage>
                  </software>

                  <!--Application guest hostname: Update hostname-->
                  <serverinfo>
                      <hostname>jesco</hostname>
                  </serverinfo>
                  <scripts>
                      <presrvapp>
                         <scriptfile id="appInt">
                              <filename>/usr/TKLC/plat/bin/netAdm</filename>
                              <arguments>set --device=int --address=10.254.254.4 --netmask=255.255.255.224 --
onboot=yes --bootproto=none</arguments>
                          </scriptfile>
```

```
                        <!--Application Guest xmi network: Update address and netmask-->
                        <scriptfile id="appXmi">
                            <filename>/usr/TKLC/plat/bin/netAdm</filename>
                            <arguments>set --device=xmi --address=10.250.51.186 --netmask=255.255.255.0 --
onboot=yes --bootproto=none</arguments>
                        </scriptfile>

                        <!--Application Guest xmi default route: Update gateway-->
                        <scriptfile id="appRoute">
                            <filename>/usr/TKLC/plat/bin/netAdm</filename>
                            <arguments>add --route=default --device=xmi --gateway=10.250.51.1</arguments>
                        </scriptfile>
                    </presrvapp>
                    <postdeploy>
                       <!--Sleep allows time for mediation scripts completion-->
                       <scriptfile id="appSleep">
                           <filename>/bin/sleep</filename>
                           <arguments>60</arguments>
                        </scriptfile>
                       <!--Application Post Deploy Configuration Script-->
                       <scriptfile id="appConfig">
                           <filename>/opt/xIH/apps/install.sh</filename>
                           <timeout>3000</timeout>
                        </scriptfile>
                    </postdeploy>
                </scripts>
            </tvoeguest>
        </servers>
          </fdc>
```

Appendix B

Adding ISO Images to the PM&C Image Repository

Topics:

Adding ISO Images to the PM&C Image Repository

Note: If the ISO image has already been added to the PM&C Software Inventory in a previous procedure, skip this procedure.

This procedure provides the steps for adding ISO images to the PM&C repository.

1. Make the image available to PM&C

There are three 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.
- Attach the USB device containing the ISO image to a USB port of the Management Server.
- Use sftp to transfer the iso image to the PM&C server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
  - cd into the directory where your ISO image is located (not on the PM&C server)
  - Using sftp, connect to the PM&C management server

```
> sftp pmacftpusr@<pmac_management_network_ip>
> put <image>.iso
```

  - After the image transfer is 100% complete, close the connection

```
> quit
```

Refer to the documentation provided by application for pmacftpusr password.

PM&C GUI: Login

Open web browser and enter:

```
https://<pmac_management_network_ip>
```

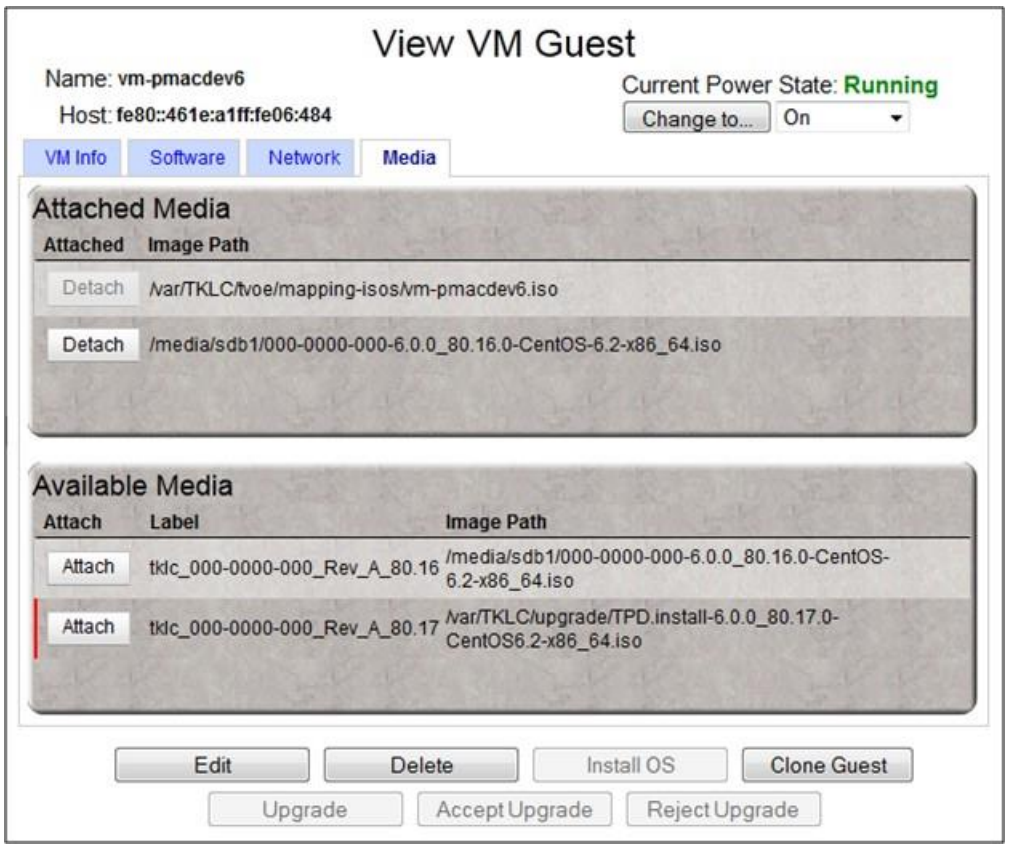
Login as pmacadmin user.

PM&C GUI: Attach the software image to the PM&C guest

If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step.

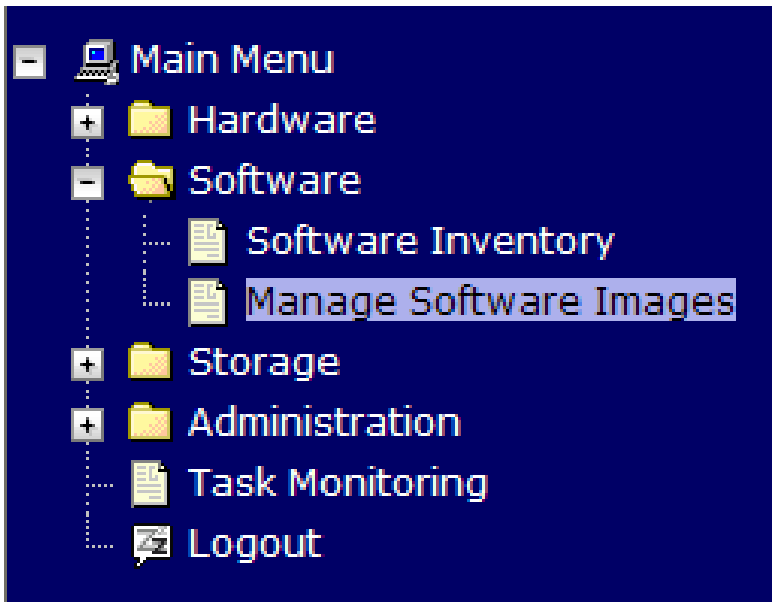
In the PM&C GUI, navigate to **Main Menu ➢ VM Managmenet.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.

Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button. After a pause, the image will appear in the "**Attached Media**" list.



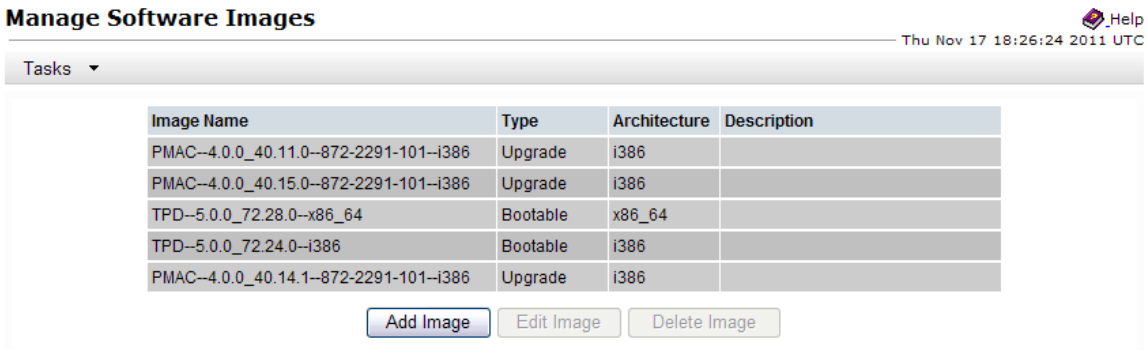
1. **PM&C GUI:** Navigate to Manage Software Images

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



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

Press the **Add Image** button .

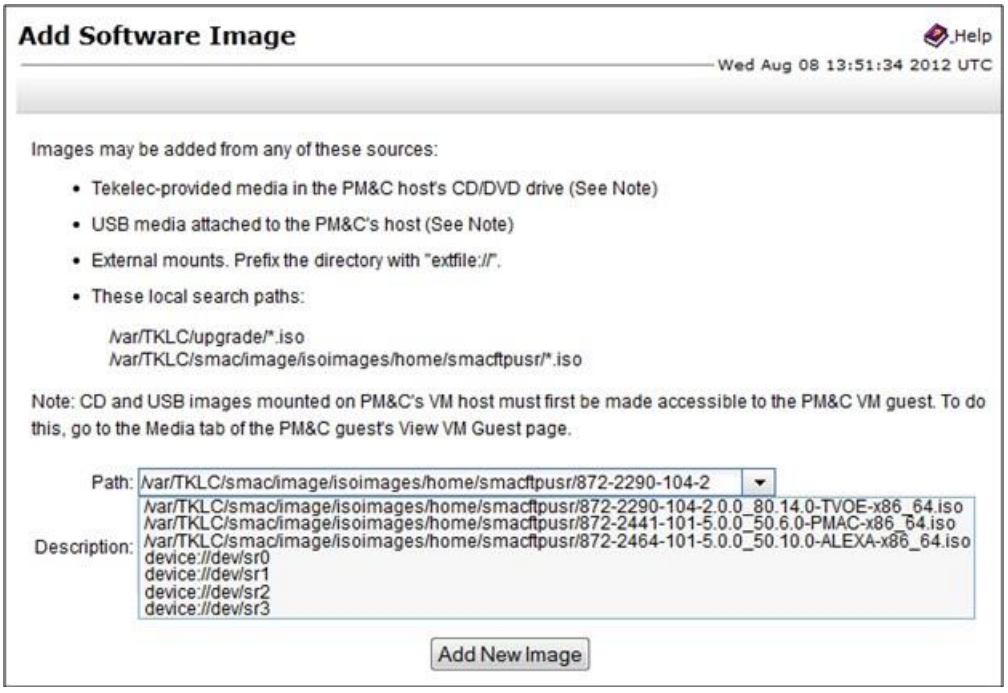


3. **PM&C GUI:** Add the ISO image to the PM&C image repository.

   Select an image to add:

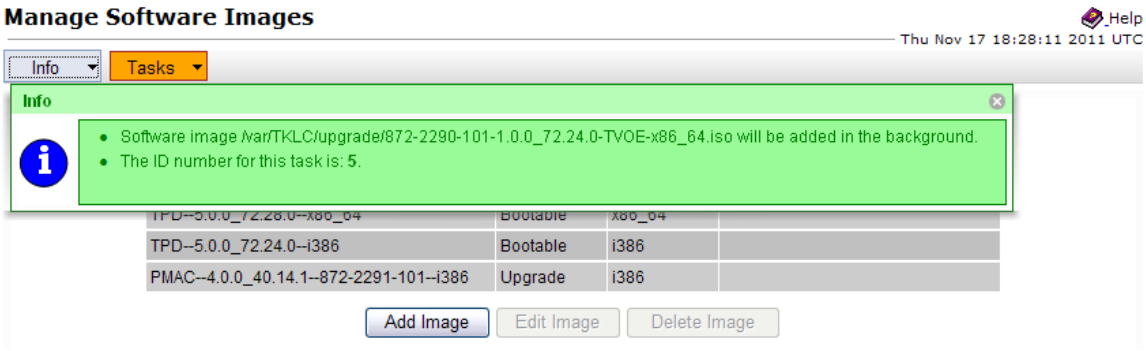
   - If in Step 1 the image was transferred to PM&C via sftp it will appear in the list as a local file "/var/TKLC/...".
   - If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number.

   Enter an appropriate image description and press the **Add New Image** button.



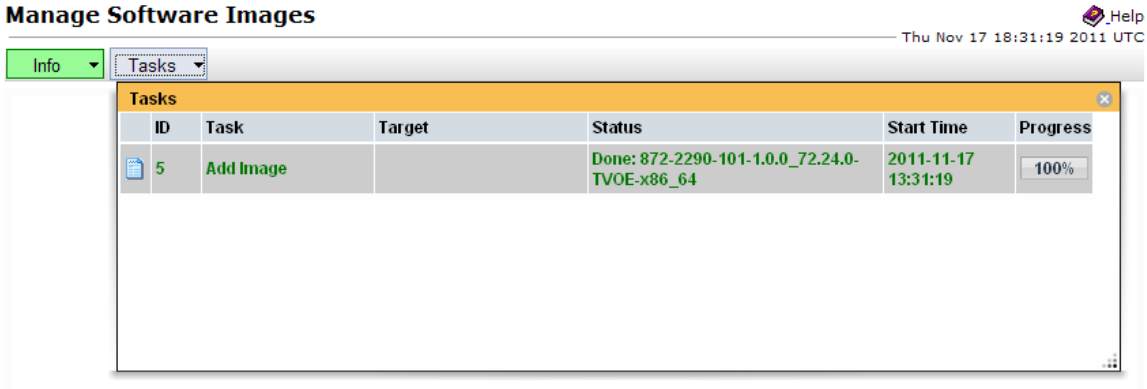
4. **PM&C GUI** Monitor the Add Image status

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



5. **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%". Check that the correct image name appears in the Status column:



6. **PM&C GUI:** Detach the image from the PM&C guest

   If the image was supplied on CD or USB, return to the PM&C guest's "**Media**" tab used in Step 3, locate the image in the "**Attached Media**" list, and click its "**Detach**" button. After a pause, the image will be removed from the "**Attached Media**" list. This will release the virtual device for future use.

   Remove the CD or USB device from the Management Server.

   Note: If there are additional ISO images to be provisioned on the PM&C, repeat the procedure with the appropriate ISO image data.

Appendix C

External Drive Removal Procedure

Topics:

External Drive Removal Procedure

Note: The IDIH virtual guests must be deleted before you perform this procedure. Login into the PM&C GUI to delete the virtual guests.

Warning: Do not perform this procedure on an IDIH system unless you intend to do a fresh TVOE installation. This procedure will destroy all of the Data in the Oracle Database!

1. Login into the PM&C GUI as pmacadmin and delete the oracle, mediation and application guests.

   a) VM Management -> Select Guest Oracle, Mediation or Application -> Delete

2. As admusr user on the TVOE host, verify the external drive exists. If you are performing this procedure on a HP Blade use slot address 3. If you are performing this procedure on a HP RMS use slot address 2.

```
HP BL460 Blade Example:
[admusr@demo2 ~]# sudo hpacucli ctrl slot=3 ld all show

Smart Array P410i in Slot 3

   array A

      logicaldrive 1 (3.3 TB, RAID 1+0, OK)

HP DL380 Gen8 RMS Example:
[admusr@d-ray ~]# sudo hpacucli ctrl slot=2 ld all show

Smart Array P420 in Slot 2

   array A

      logicaldrive 1 (1.1 TB, RAID 1+0, OK)

Netra X3 Example:
[admusr@corsair ~]$ sudo megacli -ldinfo -l1 -a0 | head


Adapter 0 -- Virtual Drive Information:
Virtual Drive: 1 (Target Id: 1)
Name                :
RAID Level          : Primary-1, Secondary-0, RAID Level Qualifier-0
Size                : 1.633 TB
Mirror Data         : 1.633 TB
State               : Optimal
Strip Size          : 64 KB


HP DL380 Gen9 RMS Example:
[admusr@gen9-tvoe ~]$ sudo hpssacli ctrl slot=0 ld all show

Smart Array P440ar in Slot 0 (Embedded)

   array A

      logicaldrive 1 (838.3 GB, RAID 1, OK)

   array B

      logicaldrive 2 (1.6 TB, RAID 1+0, OK)
```

3. As admusr user on the TVOE host, Remove the external drive and volume group with storageClean, Please read all prompts and answer accordingly.

   Note: Be sure to delete the Old Oracle guest if it exist. You can find and delete the oracle guest in the PM&C GUI under “vm management”.

```
HP BL460 Blade Example:
[admusr@demo2 ~]# sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=3
Called with options: hpdisk --slot=3
WARNING: This will destroy all application data on the server! Continue? [Y/N]

HP DL380 Gen8 RMS Example:
[admusr@d-ray ~]# sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=2
Called with options: hpdisk --slot=2
WARNING: This will destroy all application data on the server! Continue? [Y/N]

Netra X3 Example:
[root@hellcat ~]# sudo /usr/TKLC/plat/sbin/storageClean pool \
--poolName=external --level=pv
[root@hellcat ~]# sudo /usr/TKLC/plat/sbin/storageClean lvm \
--vgName=external --level=scrub
[root@hellcat ~]# sudo megacli -cfglddel -l1 -a0

HP DL380 Gen9 RMS Example:
[root@hellcat ~]# sudo /usr/TKLC/plat/sbin/storageClean pool \
--poolName=external --level=pv
[root@hellcat ~]# sudo /usr/TKLC/plat/sbin/storageClean lvm \
--vgName=external --level=scrub
[root@hellcat ~]# sudo hpssacli ctrl slot=0 ld 2 delete
```

HP Static High Performance Mode Procedure

Note: This procedure is only available on HP hardware.

Warning: Do not perform this procedure on an IDIH system unless you intend to do a fresh TVOE installation! Otherwise you must shutdown all guests and the TVOE host gracefully to avoid Data Corruption.

1. Login into the HP ILO .

   a) Launch the Java Intergrated Remote Console.

   b) Select Power Switch, then Select Reset.

   c) Wait for the ProLiant System Bios Prompt

   d) Select F9 for setup.

e) Once the Bios menu becomes available

f) Select “Power Management Options”, then select “HP Power Regulator” and select “HP Static High Performance Mode”.

g) Exit bios and save your bios setttings.

Appendix D

IDIH Network Hardware Installation Worksheets

Topics:

Config File Option: idihRmsPmacSingle.xml

Rack mount server element
RMS ID:_____ ILO Address: _____ RMS name:_____
Cabinet HW ID:_____
TVOE Host element
TVOE host ID:_____ RMS Hardware ID:_____
TVOE hostname:_____
NTP servers
ntpserver1 IP:_____ ntpserver2 IP:_____
TVOE XMI interface
Device:_____ VLAN ID:_____
TVOE IMI interface
Device:_____ VLAN ID:_____
TVOE Management Bridge
Interface:_____ IP Address:_____ Netmask:_____
gateway:_____
TVOE IMI Bridge
Interface:_____
Oracle Guest
Hostname:_____
Management IP Address:_____ Netmask:_____
gateway:_____
Mediation Guest
Hostname:_____
Management IP Address:_____ Netmask:_____
gateway:_____
IMI IP Address:_____ Netmask:_____
Application Guest
Hostname:_____
Management IP Address:_____ Netmask:_____ gateway:_____

Config File Option: idihRmsPmacMulti.xml

Rack mount server element

RMS ID:_____ ILO Address: _____ RMS name:_____ Cabinet HW ID:_____

TVOE Host element

TVOE host ID:_____ RMS Hardware ID:_____ TVOE hostname:_____

NTP servers

ntpserver1 IP:_____ ntpserver2 IP:_____

TVOE XMI interface

Device:_____ VLAN ID:_____ Bond Interfaces :_____

TVOE IMI interface

Device:_____ VLAN ID:_____

TVOE Management Bridge

Interface:_____ IP Address:_____ Netmask:_____ gateway:_____

TVOE IMI Bridge

Interface:_____

Oracle Guest

Hostname:_____

Management IP Address:_____ Netmask:_____ gateway:_____

Mediation Guest

Hostname:_____

Management IP Address:_____ Netmask:_____ gateway:_____

IMI IP Address:_____ Netmask:_____

Application Guest Hostname:_____

Management IP Address:_____ Netmask:_____ gateway:_____

IDIH RMS Installation stand-alone Single Uplink

Config File Option: idihRmsSingle.xml

Rack mount server element
RMS ID:_____ ILO Address: _____ RMS name:_____
Cabinet HW ID:_____
TVOE Host element
TVOE host ID:_____ RMS Hardware ID:_____
TVOE hostname:_____
NTP servers
ntpserver1 IP:_____ ntpserver2 IP:_____
TVOE XMI interface
Device:_____ VLAN ID:_____
TVOE IMI interface
Device:_____ VLAN ID:_____
TVOE XMI Bridge
Interface:_____ IP Address:_____ Netmask:_____
gateway:_____
TVOE IMI Bridge
Interface:_____
Oracle Guest
Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____
Mediation Guest
Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____
IMI IP Address:_____ Netmask:_____
Application Guest
Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____

Config File Option: idihRmsMulti.xml

Rack mount server element
RMS ID:_____ ILO Address: _____ RMS name:_____
Cabinet HW ID:_____
TVOE Host element
TVOE host ID:_____ RMS Hardware ID:_____
TVOE hostname:_____
NTP servers
ntpserver1 IP:_____ ntpserver2 IP:_____
TVOE XMI interface
Device:_____ VLAN ID:_____ Bond Interfaces :_____
TVOE IMI interface
Device:_____ VLAN ID:_____
TVOE XMI Bridge
Interface:_____ IP Address:_____ Netmask:_____
gateway:_____
TVOE IMI Bridge
Interface:_____
Oracle Guest
Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____
Mediation Guest
Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____
IMI IP Address:_____ Netmask:_____
Application Guest
Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____

IDIH Blade Installation Single Uplink

Config File Option: idihBladeSingle.xml

Enclosure Element

Enclosure ID:_____ Cabinet HW ID:_____ OA1 IP:_____
OA2 IP:_____

Blade Element

Blade ID:_____ Enclosure HW ID:_____ Bay:_____

TVOE Host element

TVOE host ID:_____ RMS Hardware ID:_____
TVOE hostname:_____

NTP servers

ntpserver1 IP:_____ ntpserver2 IP:_____

TVOE XMI interface

Device:_____ VLAN ID:_____

TVOE IMI interface

Device:_____ VLAN ID:_____

TVOE XMI Bridge

Interface:_____ IP Address:_____ Netmask:_____
gateway:_____

TVOE IMI Bridge

Interface:_____

Oracle Guest

Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____

Mediation Guest

Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____
IMI IP Address:_____ Netmask:_____

Application Guest

Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____

Config File Option: idihBladeMulti.xml

Enclosure Element
Enclosure ID:_____ Cabinet HW ID:_____ OA1 IP:_____
OA2 IP:_____
Blade Element
Blade ID:_____ Enclosure HW ID:_____ Bay:_____
TVOE Host element
TVOE host ID:_____ RMS Hardware ID:_____
TVOE hostname:_____
NTP servers
ntpserver1 IP:_____ ntpserver2 IP:_____
TVOE XMI interface
Device:_____ VLAN ID:_____ Bond Interfaces :_____
TVOE IMI interface
Device:_____ VLAN ID:_____
TVOE XMI Bridge
Interface:_____ IP Address:_____ Netmask:_____
gateway:_____
TVOE IMI Bridge
Interface:_____
Oracle Guest
Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____
Mediation Guest
Hostname:_____
XMI IP Address:_____ Netmask:_____ gateway:_____
IMI IP Address:_____ Netmask:_____
Application Guest
Hostname:_____

XMI IP Address:_____
Netmask:_____
gateway:_____

APPENDIX E: MY ORACLE SUPPORT (MOS)

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

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

When calling, there are multiple layers of menus selections. Make the selections in the sequence shown below on the Support telephone menu:

1) For the first set of menu options, select 2, “New Service Request”. You will hear another set of menu options.
2) In this set of menu options, select 3, “Hardware, Networking and Solaris Operating System Support”. A third set of menu options begins.
3) In the third set of options, select 2, “Non-technical issue”. Then you will be connected to a live agent who can assist you with MOS registration and provide Support. Identifiers. Simply mention you are a Tekelec Customer new to MOS.