Oracle® Communications
Performance Intelligence Center
Patch Installation Guide
Release 10.2.1
E77488-01

June 2017
Table of Contents

Chapter 1: About This Help Text .................................................................................................................. 5
  Scope And Audience ................................................................................................................................. 5
  Related Publications ................................................................................................................................. 5
  Requirements and Prerequisites................................................................................................................ 5
    Hardware Requirements .......................................................................................................................... 5
    Software Requirements ........................................................................................................................... 5
  Reference Documents .................................................................................................................................. 7

Chapter 2: Patch Installation Overview Flowcharts .................................................................................. 8
  Flowchart Description ................................................................................................................................ 8
  Management Patch Installation .................................................................................................................. 9
  Probed and Integrated Acquisition Patch Installation ............................................................................... 10
  Mediation Patch Installation ..................................................................................................................... 11
  Protocol Patch Installation ........................................................................................................................ 12

Chapter 3: Patching Back out Overview .................................................................................................... 13
  Management Patching Back out ................................................................................................................ 13
  Acquisition Patching Back out .................................................................................................................. 13
  Mediation Patching Back out ...................................................................................................................... 13

Chapter 4: Health check ............................................................................................................................ 14
  Mediation Subsystem Health check ........................................................................................................ 14
  Acquisition Health check ......................................................................................................................... 15
  Management Pre-Upgrade Health check and Settings.......................................................................... 16
    Pre-upgrade health check for Management Server ............................................................................... 16
  Check Management Backup is valid ........................................................................................................ 17
  Upgrade Configurations using Deprecated Field(s) .............................................................................. 17
  Global Health check ................................................................................................................................ 18
    iLO Access ........................................................................................................................................... 18
    System Cleanup .................................................................................................................................... 18
    Engineering Document .......................................................................................................................... 18
    Troubleshooting Session Status ........................................................................................................... 18
    Systems Alarms ................................................................................................................................... 19
    Alarm Forwarding ................................................................................................................................. 19
Chapter 5: Management Patch Installation ........................................... 20
management Pre-Upgrade Check .......................................................... 20
Upgrade Management Server ............................................................... 23
Post-Upgrade Settings .......................................................................... 24
Management Post-Upgrade Check ......................................................... 27
Post Upgrade ......................................................................................... 28
Management Backup ............................................................................ 28
Unset Configuration on Management (onebox) ....................................... 28
Chapter 6: Acquisition Patch Installation ............................................. 29
Acquisition Upgrade .............................................................................. 29
Sync Management with Acquisition ..................................................... 29
Chapter 7: Mediation Patch Installation ............................................... 31
Mediation Subsystem ............................................................................ 31
Upgrade DTO Package ........................................................................ 32
Chapter 8: Protocol Upgrade ............................................................... 33
Upload Mediation Protocol ISO to Management .................................. 33
Centralized Mediation Protocol Upgrade .............................................. 33
Appendix A: My Oracle Support ......................................................... 34
List of Figures
Figure 1. Management Patch Installation ........................................... 9
Figure 2. Acquisition Patch Installation .............................................. 10
Figure 3. Mediation Patch Installation ............................................... 11
Figure 4. Protocol Patch Installation .................................................. 12
Chapter 1: About This Help Text

Scope And Audience
This document describes the patch installation procedures for the "Oracle Communications Performance Intelligence Center" system at Release 10.2.1

This document is intended for use by trained engineers in software installation on both Oracle and HP hardware. A working-level understanding of Linux, Oracle Database 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, 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 Patch Installation Overview chapter that provide the sequence of the procedures for each component of the system to upgrade. Each procedure describes a discrete action. It is expected that the individuals responsible for patching the system should reference these flowcharts during this upgrade process.

Related Publications
Please refer to MOS Information Center: Upgrade Oracle Communications Performance Intelligence Center 1984685.2

Requirements and Prerequisites

Hardware Requirements
Refer document Hardware Guidelines (see chapter Reference Documents).

Software Requirements
The following software is required for Performance Intelligence Center 10.2.1 Patch Installation.

Take in consideration you might need also the software from the installed release in case you would have to proceed a disaster recovery. Refer to Maintenance Guide of the release 10.2.1 for detailed instruction.

Note: For specific versions and part numbers, see the MOS Information Center: Upgrade Oracle Communications Performance Intelligence Center 1984685.2.

The following software is required for the patch installation.

Oracle Communication GBU deliverables:

• Management Server
• Mediation Server
• Mediation Protocol
• Acquisition Server
• TADAPT
• TPD
All the software must be downloaded from Oracle Software Delivery Cloud (OSDC)

https://edelivery.oracle.com/

Please refer to KM notes which are constantly updated with last improvements:

<table>
<thead>
<tr>
<th>Title</th>
<th>MOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Oracle Communications Performance Intelligence Center, is providing some guidances</td>
<td>KM_1984685.2</td>
</tr>
<tr>
<td>Patches for Oracle Communications Performance Intelligence Center</td>
<td>KM_1989320.2</td>
</tr>
<tr>
<td>Management Server (NSP) on Third-Party Server Installation Guide for Performance Intelligence Center Products</td>
<td>KM_2164544.1</td>
</tr>
<tr>
<td>Management Server (NSP) on TPD system Installation Guide for Performance Intelligence Center Products</td>
<td>KM_2251899.1</td>
</tr>
<tr>
<td>Capacity management good practices</td>
<td>KM_1683859.2</td>
</tr>
</tbody>
</table>

In case of engineered system like ODA and ZFS the upgrade of its software is not mandatory, however in case customer want to update ODA or ZFS software following information can be used:

- ODA
  - Oracle Database Appliance - 12.1.2 and 2.X Supported ODA Versions & Known Issues [KM_888888.1](#)
  - As reminder, the initial installation documentation is there [Database Appliance Getting Started Guide](#)

- ZFS
  - Oracle ZFS Storage Appliance: Software Updates [KM_2021771.1](#)
  - As reminder, the initial installation documentation is there [ZFS Storage Appliance Installation Guide](#) and [ZFS Storage Appliance Administration Guide](#)
Reference Documents

[3] HP Solutions Firmware Upgrade Pack, choose the more recent one
[5] Installation Guide, Performance Intelligence Center release 10.2.1
[7] Hardware Guidelines, Performance Intelligence Center release 10.2.1
[8] MOS Information Center: Upgrade Oracle Communications Performance Intelligence Center 1984685.2
[9] Upgrade Guide, Performance Intelligence Center release 10.2.1

Performance Intelligence Center release 10.2.1 is using Comcol 7.3 with TPD 7.4
Chapter 2: Patch Installation Overview Flowcharts

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

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.

It is recommended to upgrade the firmware needs to the latest Oracle supported levels for all hardware components, however this firmware upgrade is not mandatory. The system on the source release also need to have installed all necessary patches applicable to source release prior the patch installation.
Management Patch Installation
This flowchart depicts the sequence of the upgrade procedure to apply for the patch installation on the Management server setup.

Figure 1. Management Patch Installation
Probed and Integrated Acquisition Patch Installation

This flowchart depicts the sequence of upgrade procedure that must be executed to install the patch on standalone Probed/Integrated Acquisition Server.

For a Standalone Acquisition server, only PMF is to be updated (refer flowchart).

For Integrated Acquisition Sub-system, depending on the number of servers in a sub-system, the required procedures depicted in the flowchart will need to be repeated.

Figure 2. Acquisition Patch Installation
Mediation Patch Installation

This flowchart depicts the sequence of procedures that must be executed to upgrade the Mediation subsystem and associated server functions. The procedure is triggered from one server in the subsystem and runs in parallel on all servers in the subsystem.

**Note:** Some of the xDR/KPI sessions are stored on different servers in the Data Record Storage pool. As Centralized Mediation Protocol upgrade is analyzing all session that are configured on particular Mediation subsystem, all Oracle servers where those sessions are stored must be accessible. Otherwise Centralized Mediation Protocol upgrade will fail.

**Figure 3. Mediation Patch Installation**
Protocol Patch Installation

This flowchart depicts the sequence of procedures that must be executed to upgrade the Protocols.

Figure 4. Protocol Patch Installation
The back out is designed to come back to the previous situation and is applicable only in case of successful upgrade. The back out sequence would be similar to the upgrade sequence starting with Management, then Acquisition, and Mediation.

**Management Patching Back out**
Management application patching back out is implemented as a Disaster Recovery procedure. Follow the Management Disaster Recovery Procedure, described in the Maintenance Guide.

**Acquisition Patching Back out**
Acquisition application patching back out is implemented as a Disaster Recovery procedure. Follow the Acquisition Disaster Recovery Procedure, described in the Maintenance Guide.

**Mediation Patching Back out**
Mediation application patching back out is implemented as a Disaster Recovery procedure. Follow the Mediation Disaster Recovery Procedure, described in the Maintenance Guide.
Mediation Subsystem Health check

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

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

2. As cfguser, run:

   ```
   $ analyze_subsystem.sh
   ```

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

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

   Example of overall output:

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

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

Acquisition Health check

This procedure describes how to run the health check script on Acquisition servers. The script gathers the health check information from each server in the Acquisition subsystem or from standalone server. The script should be run from each of the server of the Acquisition subsystem or on stand-alone. The output consists of a list of checks and results, and, if applicable, suggested solutions.

1. Run analyze_server.sh script as cfguser:
   
   ```bash
   $ analyze_server.sh -i
   ```

2. Analyze the output of the script for errors. Issues reported by this script must be resolved before any further usage of this server. Verify no errors are present.
   
   If the error occurs, refer to Appendix A: My Oracle Support

Example output for a healthy subsystem:

```
04:57:30: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
04:57:31: date: 02-26-16, hostname: imf9040-1a
04:57:31: TPD VERSION: 7.0.3.0.0-86.40.0
04:57:31: XMF VERSION: [ 10.2.0.0.0-24.1.0 ]
04:57:32: -------------------------------------------------
04:57:32: Checking disk free space
04:57:32:       No disk space issues found
04:57:32: Checking syscheck - this can take a while
04:57:43:       No errors in syscheck modules
04:57:44: Checking statefiles
04:57:44: Statefiles do not exist
04:57:44: Checking runlevel
04:57:45:       Runlevel is OK (4)
04:57:45: Checking upgrade log
04:57:45: Install logs are free of errors
04:57:45: Analyzing date
04:57:46:       NTP deamon is running
04:57:46:       IP of NTP server is set
04:57:46:       Server is synchronized with ntp server
04:57:47: Analyzing IDB state
04:57:47:       IDB in START state
04:57:47: Checking IDB database
04:57:48: aud it has not found any errors
04:57:48: Analyzing processes
04:57:49: Processes analysis done
04:57:49: Analysing database synchronization
04:57:50: Either Database synchronization in healthy state or errors found are non-blocking
04:57:50: Checking weblogic server entry
04:57:50: Appserver is present
04:57:50: All tests passed. Good job!
04:57:51: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
```
Management Pre-Upgrade Health check and Settings

Pre-upgrade health check for Management Server

1. Pre-Upgrade Verification

   It is needed to reset the tekelec and TklcSrv password to default. Some python scripts need to have default password, the scripts are needed for deploying the scheduler queues and other resources. The historical KPI application has dependencies on the scheduler queues.

   a) Please verify the system User Password is Default Password.
   b) Please Change the tekelec User Password to Default Password.

   **Steps to change tekelec user Password**

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

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

   c) Please Change the TklcSrv User Password to Default Password.

   **Steps to change TklcSrv user Password**

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

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

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

2. Check Weblogic console is not locked

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

   a) Connect to Weblogic console.
   http://192.168.1.1:8001/console
where 192.168.1.1 is the IP address of Management server.

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

Check Management Backup is valid

Refer to the section “Check Management Server Backup is valid” from Upgrade Guide.

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

Upgrade Configurations using Deprecated Field(s)

This step is to be performed to upgrade configurations which are using Deprecated field(s) so as to make sure none of the configuration will use Deprecated field which may get removed in later releases.

Note that a patch was never introducing new deprecated field and this procedure should be rarely necessary.

1. Login to Management application interface as TklcSrv user.
2. Click Upgrade Utility
3. Click Dictionaries with Deprecated Field(s) link on home page, this will a list of dictionaries having deprecated field(s).
4. Select any one of the dictionaries and choose View Dependent Configurations icon from tool bar. This will display list of KPIs, Queries and Filters using deprecated fields. You can also export this list by clicking on Export button given on that popup. If there are no dependent configurations then this list will be empty.

Take care to check each Tab and not Only the default one KPI.

The Screen shot bellow shows an example where the job has not been done at the end of the previous upgrade.
Global Health check

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

System Cleanup
Discuss with the customer to clean up the system as much as possible in order to reduce the risk and avoid any issue due to some objects that would no more be used.

Engineering Document
Make sure you get the latest available engineering document and it is up to date. The latest version should be documented on the Customer Info Portal, as well as the current password for the admin users

Troubleshooting Session Status
Navigate from the home screen to Troubleshooting
NOTE: Look for any sessions that are lagging behind the current time.
1. View All records
2. Filter by end date
3. Screen capture the information
Verify which sessions are lagging. Statistics sessions must also be considered but take in consideration records are periodically generated.
Try to access the session it-self and check the session content and especially make sure the PDU are properly recorded.
**Systems Alarms**

Access the system alarm and fix all alarms on the system. In case some alarms can’t be fixed due to overloaded system for example, the remaining alarms before the upgrade must be captured in order to compare with the alarms we would get at the end of the upgrade.

**Alarm Forwarding**

Connect on Management Primary and Navigate in platcfg menu to check the SNMP and SMTP configuration. Make sure the SNMP and SMTP configuration are up to date in the Engineering Document.

**KPI**

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

**Dashboard**

Access to Dashboard Application and check each dashboard is working fine

**Mediation Data Feed**

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

**Browser Export Scheduler**

Access to the Browser Export Scheduler and check the scheduled tasks configured are working as expected.
Make sure each task is documented in the Engineering Document.

**Capacity Management**

Access Troubleshooting and open CapacityManagement UsageStats session to verify if normal activity is monitored hourly for probed acquisition, integrated acquisition, mediation and mediation protocol.
Chapter 5: Management Patch Installation

Management Pre-Upgrade Check

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

2. Pause JMS and Purge terminated alarm

   Note: Weblogic 12.2.1.0.0 has a bug (Bug 22481818) affecting JMS module. So, in order to fix it you need to apply a patch: Patch 21830665

   a) Connect to Weblogic console in order to check JMS consumption.

   In the Services section, go to messaging and then JMS Servers menu:
For Each JMS servers, click on the name of the server and then to the menu Control:

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

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

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

   a) As root run:
   
   ```bash
   # df -kh /opt/oracle/backup
   ```
   
   Example output:
   
<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/cciss/c0d2p1</td>
<td>67G</td>
<td>11G</td>
<td>57G</td>
<td>16%</td>
<td>/opt/oracle/backup</td>
</tr>
</tbody>
</table>
   
   b) Check the space available under Avail column of this table. This should be at least 15-20 GB approx. e.g. in above table shown total space available is 57GB.

   **Note:** If total available space is less than 2 GB, then do not continue with upgrade. refer to Appendix A: My Oracle Support.

4. **Generate the “Bulk Export Configurations” and “Create Configuration Report”**

   Go to the Centralized Configuration home page and click on the link to generate this files. Keep it in a safe place on your laptop in the worst case where even a disaster recovery would not work with would help you to get in information, in order to re-create the configuration.

5. **Synchronize the Integrated Acquisition**

   Go to the Centralized Configuration and synchronize the Integrated Acquisition in the acquisition part before to start any operation in order to avoid discovering new links while the upgrade. Proceed to an “Apply changes” if some are to do.

   Take care if the Custom Name Override feature is enable on the link set, the names would be replaced by the one used on the Eagle.

   The function is available on the Linksets list page tool bar.

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

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

   a) As root run:
   
   ```bash
   # df -kh /opt/oracle/backup
   ```
   
   Example output:
   
<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/cciss/c0d2p1</td>
<td>67G</td>
<td>11G</td>
<td>57G</td>
<td>16%</td>
<td>/opt/oracle/backup</td>
</tr>
</tbody>
</table>
   
   b) Check the space available under Avail column of this table. This should be at least 15-20 GB approx. e.g. in above table shown total space available is 57GB.

   **Note:** If total available space is less than 2 GB, then do not continue with upgrade. refer to Appendix A: My Oracle Support.

4. **Generate the “Bulk Export Configurations” and “Create Configuration Report”**

   Go to the Centralized Configuration home page and click on the link to generate this files. Keep it in a safe place on your laptop in the worst case where even a disaster recovery would not work with would help you to get in information, in order to re-create the configuration.

5. **Synchronize the Integrated Acquisition**

   Go to the Centralized Configuration and synchronize the Integrated Acquisition in the acquisition part before to start any operation in order to avoid discovering new links while the upgrade. Proceed to an “Apply changes” if some are to do.

   Take care if the Custom Name Override feature is enable on the link set, the names would be replaced by the one used on the Eagle.

   The function is available on the Linksets list page tool bar.
Upgrade Management Server

1. Upgrade Management Server
   a) Login as root user on terminal console of Management server.
   b) Copy the Management ISO on server.
   c) Mount the ISO file
      
      ```
      # mount -o loop iso_path /mnt/upgrade
      
      where iso_path is the absolute path of the Management ISO image, which includes the name of the image (for example, /var/ORCL/iso_file_name.iso).
      ```
   d) As root, run:
      ```
      # /mnt/upgrade/upgrade_nsp.sh
      ```
      Note: Run this procedure via iLO or through any disconnectable console only.
   e) Wait for Management upgrade to get complete. Remove this file to save disk space.
      As root, run:
      ```
      # rm -f /var/ORCL/iso_file
      ```
      where iso_file is the absolute path of the ISO image, which includes the name of the image.
      After the installation the server will restart automatically. Log back in and review the Management installation log (/var/log/nsp/install/nsp_install.log). If Management did not install successfully, contact MOS
Post-Upgrade Settings

1. Resume JMS Consumption

   On Management Standard Server the JMS consumption must be resumed from weblogic console.

   **Note:** Weblogic 12.2.1.0.0 has a bug (Bug 22481818) affecting JMS module. So, in order to fix it you need to apply a patch: [Patch 21830665](#)

   a) Connect to Weblogic console in order to check JMS consumption.

   ![Weblogic Console Screenshot]

   In the Services section, go to messaging and then JMS Servers menu:
For Each JMS servers, click on the name of the server and then to the menu Control:

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

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

2. **Restrict access of Management frontend to HTTPS (Mandatory)**
   This action must be done manually and not from installation script as the Apache server is not available in Oracle Linux as it was with TPD based platform.
   **Disable access to HTTP**
   - a. Open a terminal console and Login as a root user on Management Server One-Box server
   - b. Edit `/etc/httpd/conf/httpd.conf` file and search for line “Listen 80”
   - c. Remove the line “Listen 80”
   - d. Restart httpd daemon

   ```bash
   /bin/systemctl restart httpd.service
   ```

3. **Configure host file for Mail Server (Optional)**
   This configuration is optional and required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined and no server address override defined by app).
   1. Open a terminal window and log on as root on Standard Server
   2. Edit hosts file and make an entry of mail.server as shown below:

   ```
   # vi /etc/hosts
   10.248.18.4 mail.server
   ```
Output of hosts file will be similar as shown below. Replace 10.248.18.4 with your mail server IP

```
# cat /etc/hosts
127.0.0.1 localhost
10.248.18.4 mail.server
```

4. **Transfer Ownership of TklcSrv object**
   **Note:** Follow the steps only if some object belonging to TklcSrv were created in previous version. The ownership is transferred back to other user from TkIcsrv post upgrade. This action is present as a precautionary procedure and not a mandatory one.
   a) Open a web browser and log in to the Management application interface TklcSrv user.
   b) Navigate to **security application** ☀ Transfer ownership value
   c) Transfer all the TklcSrv object to and other user (tekelec for example)

**Management Post-Upgrade Check**

**Box:** must be done from a browser (IE/Mozilla).
This procedure describes the steps for the Sanity Tests of Management.

1. **WebLogic Console**
   From Internet Explorer, connect to the WebLogic console using the following URL:
   `http://192.168.1.1:8001/console`
   where 192.168.1.1 is the IP address of the Management Server (In case of One-box configuration)

2. **Login**
   You should be prompted to “Log in to work with the WebLogic Server domain “. Connect with User weblogic

3. **Console Display**
   Under the **Environment** heading, click on the “**Servers**”.

4. **Health Check**
   a) On clicking the “Servers” link in the last step, the console would display the **Summary of Servers**, with a list of the three servers, nsp1a, nsp1b and nspadmin (In case of One-box configuration)
   b) Entries in the columns **State** and **Health** should be **RUNNING** and **OK** for all three servers (In case of One-box configuration)

5. **Management GUI**
   From Internet Explorer, connect to the Management Application GUI using the following URL:
   `http://192.168.1.1/`
   where 192.168.1.1 is the IP address of the Management Server (in case of One-box configuration)

6. **Login**
   Login to the Application with User name **tekelec**

7. **Portal**
   a) In the top frame, on mouse-over on the link **Portal**, click on the **About** link that will be displayed.
   b) A pop-up window with the build information will be displayed.

8. **Build Verification**
   The build version should display “Portal 10.2.1-X.Y.Z”. Where 10.2.1-X.Y.Z should be the new build number.
Post Upgrade

1. Open a terminal window and log in as root on the Management.
2. As root, run:
   ```
   # /opt/nsp/scripts/procs/post_upgrade_sanity_check.sh
   ```
3. Review the Management installation logs (`/var/log/nsp/install/nsp_install.log`). Verify the following:
   - Oracle server health is OK
   - WebLogic health for ports 5556, 7001, 8001 is OK

Management Backup

Refer section Management Server Backup from Upgrade Guide, doc ID E77487-01.

Note: For Patch Installation, please ignore the step to disable crontab entry for launch_pic_global_backup.sh.

Unset Configuration on Management (onebox)

Unset configuration application access restriction automatically set during Management upgrade by performing the below steps.

Note: Configuration application are automatically restricted to TklcSrv and tekelec user during Management upgrade. After required reconfiguration, Management shall return to normal.

1. Open a web browser and log in to the NSP application interface as TklcSrv user.
2. Navigate to security application Filter access
3. Select None for Restricted configuration setting.
4. Apply modification.
Chapter 6: Acquisition Patch Installation

Acquisition Upgrade

**CAUTION:** Please perform step2 using ILO or any non-disconnectable media..

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

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

3. **Upgrade completed**
   The server will reboot and after the reboot, login prompt will be displayed.

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

Sync Management with Acquisition

1. **Apply Changes Acquisition**
   a) To Apply Changes for each subsystem go to Acquisition ☯ Sites ☯ XMF.
   b) Right click on subsystem and click on **Apply Changes** option on menu.

2. **Test the VIP function.**
   a) After sync from Management, the VIP will be available to access the active master server in the site. In order to verify the VIP setup please login to any server in the subsystem and execute the `iFoStat` command. As `cfguser` run:
      ```bash
      $ iFoStat
      ```
   Example of correct output:
### Result of Query 10.236.2.79 for Failover Status

<table>
<thead>
<tr>
<th>name</th>
<th>state</th>
<th>loc</th>
<th>role</th>
<th>mGroup</th>
<th>assg</th>
<th>HbTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMF-1a</td>
<td>IS</td>
<td>1A</td>
<td>ActMaster</td>
<td>sde_m2pa</td>
<td>7</td>
<td>2009-06-19 23:14:08</td>
</tr>
<tr>
<td>IMF-1b</td>
<td>IS</td>
<td>1B</td>
<td>StbMaster</td>
<td>sde_stc</td>
<td>6</td>
<td>2009-06-19 23:14:06</td>
</tr>
<tr>
<td>IMF-1c</td>
<td>IS</td>
<td>1C</td>
<td>Slave</td>
<td></td>
<td>0</td>
<td>2009-06-19 23:14:06</td>
</tr>
</tbody>
</table>

b) The state should be ‘IS’ for all servers and the HbTime time should be updated every few seconds.
Chapter 7: Mediation Patch Installation

Mediation Subsystem

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

1. Permit root ssh login

   On each Mediation server permit root ssh login.
   a) As root run:
      
      ```
      # /usr/TKLC/plat/sbin/rootSshLogin --permit
      ```

2. Distribute the Mediation ISO

   Note: Choose one of the servers in the subsystem. From this server you will trigger the parallel Mediation subsystem patch installation.
   Distribute the Mediation ISO file to /var/TKLC/upgrade directory using the scp command.

3. Run parallel Mediation subsystem patch installation

   Note: Run this step on where server you distributed the Mediation ISO. This step will trigger the parallel patch installation on all servers in the subsystem.
   b) As root run:
      
      ```
      # misc_upgrade_subsystem.sh –i iso_filename
      ```
      
      where iso_filename is the name of the Mediation ISO file that has been previously distributed on this server.
   c) You will be prompted to confirm the upgrade; then, you will be asked to enter the root password.
      
      The patch installation is triggered on all the servers of the subsystem.

4. Monitor parallel Mediation patch installation

   Note: The whole subsystem is upgrading now. Keep logged on the server where you have triggered the parallel upgrade, as you will see the progression. The server will reboot after successful upgrade.
   a) Once the server where you have triggered the parallel upgrade is accessible again, start monitoring script: it will apply some subsystem post-upgrade settings, after all the servers have successfully upgraded (and rebooted). As root run:
      
      ```
      # misc_upgrade_subsystem.sh --postsync
      ```
   b) You will see the regular monitoring of the upgrade progress. Keep this script running and look for successfully upgraded servers. Do not interrupt the script. Wait until the results of upgrade are shown and synchronization is restored. Monitor the script output for any errors.
      
      The logs for the upgrade must be verified at /var/TKLC/log/upgrade/upgrade.log on the server from where the upgrade is triggered. If any error appears, refer to Appendix A: My Oracle Support. The script will only finish once all servers in the subsystem have finished the upgrade.

5. Discover Mediation application in Centralized Configuration

   This procedure describes how to discover Mediation application in the Management Centralized Configuration application.
Discover all Mediation servers in Centralized Configuration application.

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

6. **Revoke root ssh login**

   **On each Mediation server revoke root ssh login.**
   a) As root run:
   
   ```bash
   # /usr/TKLC/plat/sbin/rootSshLogin --revoke
   ```

**Upgrade DTO Package**

Refer to Upgrade DTO Package from [Upgrade Guide](#).
Chapter 8: Protocol Upgrade

The protocol upgrade consists of two steps, described below, which involve procedures executed on the management server. The protocol upgrade involves upgrade of xDR builder RPM on mediation server.

Upload Mediation Protocol ISO to Management
Refer section “Upload xDR Builder ISO to Management Server” from Upgrade Guide.

Centralized Mediation Protocol Upgrade
Refer section “Install xDR Builders“ of the Upgrade Guide.
Appendix A: 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. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

MOS is available 24 hours a day, 7 days a week.