

**Oracle® Communications Performance
Intelligence Center
Maintenance Guide**

Release 10.1.5

E56062 Revision 1

August 2015

Copyright © 2003, 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notices are applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to thirdparty content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Refer to Appendix A for instructions on accessing My Oracle Support.

TABLE OF CONTENTS

TABLE OF CONTENTS	3
1 INTRODUCTION	7
1.1 DOCUMENTATION ADMONISHMENTS.....	7
1.2 REFERENCE DOCUMENTS.....	7
1.3 RELATED PUBLICATIONS	7
1.4 SCOPE AND AUDIENCE	8
1.5 REQUIREMENTS AND PREREQUISITES.....	8
1.5.1 <i>Hardware Requirements</i>	8
1.5.2 <i>Software Requirements</i>	8
2 DISASTER RECOVERY PROCEDURES ON ODA/ZFS	10
2.1 DR OF MANAGEMENT SERVER(WITH DWS DATABASE)	10
2.1.1 <i>Management Server Database recreation</i>	10
2.1.2 <i>Weblogic VMs re-deployment</i>	11
2.1.3 <i>ODA_BASE redeployment</i>	12
2.1.4 <i>ODA Physical Server Disaster</i>	13
2.2 DR OF SINGLE DWS OR MULTIPLE DWS(NO MANAGEMENT SERVER DATABASE)	13
2.2.1 <i>ODA Physical Server Disaster</i>	13
2.2.2 <i>ODA_BASE Disaster</i>	13
2.2.3 <i>DWS database re-creation</i>	14
2.3 DR OF SINGLE DWS(WITH MANAGEMENT SERVER DATABASE)	14
2.3.1 <i>ODA Physical Server Disaster</i>	14
2.3.2 <i>ODA_BASE Disaster</i>	15
2.3.3 <i>DWS database re-creation</i>	15
2.4 DR OF ZFS	15
3 MANAGEMENT SERVER DISASTER RECOVERY PROCEDURES	17
3.1 MANAGEMENT SERVER ONE-BOX HP	17
3.2 MANAGEMENT SERVER FOUR-BOX ON HP	18
3.2.1 <i>Apache Server (Four-Box)</i>	19
3.2.2 <i>Oracle Server (Four-Box)</i>	20
3.2.3 <i>Secondary WebLogic (Four-Box)</i>	21
3.2.4 <i>Primary WebLogic (Four-Box)</i>	22
3.3 MOUNT ORACLE VOLUME (RACKMOUNT ONLY)	24
3.4 REMOUNT MANAGEMENT SERVER LUN(C-CLASS BLADES ONLY)	24
3.5 MANAGEMENT SERVER PRE-INSTALL CONFIGURATION	26
3.6 INSTALL WEBLOGIC	28
3.6.1 <i>Mount Management Server media</i>	28
3.6.2 <i>Install WebLogic Product</i>	28
3.7 INSTALL ORACLE DATABASE	28
3.8 INSTALL MANAGEMENT SERVER.....	29
3.8.1 <i>Mount Management Server media</i>	29
3.8.2 <i>Install Management Server application</i>	29
3.9 RESTORE REALM BACKUP	29
3.10 RECOVER DATABASE	30

3.10.1	Recover Management Server Database on One-Box setup or ODA	30
3.10.2	Recover Management Server Database on Four-Box setup	32
3.11	MANAGEMENT SERVER POST-INSTALL SANITY CHECK (ONEBOX AND FOUR BOX)	33
4	ACQUISITION DISASTER RECOVERY PROCEDURES	35
4.1	ACQUISITION SERVER DISASTER RECOVERY.....	35
5	MEDIATION/DWS DISASTER RECOVERY PROCEDURES	36
5.1	MEDIATION/DWS DISASTER RECOVERY OVERVIEW	36
5.1.1	HP DWS server disaster recovery procedure.....	36
5.1.2	Mediation PDU Storage server disaster recovery procedure.....	37
5.1.3	Mediation Base server disaster recovery procedure.....	37
5.2	STOP IXP SERVICE	37
5.3	DISINTEGRATE SERVER WITH THE MEDIATION SUBSYSTEM	37
5.4	INTEGRATE SERVER WITH THE MEDIATION SUBSYSTEM.....	38
5.5	REMOUNT EXPORT DIRECTORIES	38
5.6	RETRIEVE LUN NUMBERS (C-CLASS BLADES ONLY).....	39
5.7	REMOUNT LUN (C-CLASS BLADES ONLY)	39
6	PIC IP CHANGES PROCEDURE.....	41
6.1	PIC IP CHANGE OVERVIEW	41
6.2	MANAGEMENT IP CHANGE PROCEDURE	41
6.2.1	Modify Management One-Box IP Address	42
6.2.2	Modify Management Apache IP Address (Four-Box Configuration).....	42
6.2.3	Modify Management Secondary or Oracle IP Address (Four-Box Configuration).....	43
6.2.4	Modify Management Primary IP Address (Four-Box Configuration)	43
6.2.5	Update Management IP addresses on xMF	43
6.2.6	Update Management IP addresses on IXP or EFS	43
6.3	ACQUISITION SUBSYSTEM IP CHANGE PROCEDURE	44
6.3.1	Change IP Addresses	44
6.3.2	Change VIP Addresses.....	44
6.3.3	Change IP Address Acquisition subsystem in Management.....	44
6.4	MEDIATION SUBSYSTEM IP CHANGE PROCEDURE.....	44
6.5	DWS IP CHANGE PROCEDURE.....	46
7	MANAGEMENT SERVER MAINTENANCE PROCEDURES	48
7.1	MANAGEMENT SERVER BACKUP PROCEDURES.....	48
7.1.1	Automatic Backup.....	48
7.1.2	Management Server Database Backup	50
7.1.3	Realm Backup	51
7.1.4	System Files Backup	51
7.2	START NSP SERVICE ON PRIMARY WHEN SECONDARY IS DOWN.....	52
7.3	START NSP SERVICE ON SECONDARY WHEN PRIMARY IS DOWN.....	52
7.4	CONFIGURE APACHE HTTPS CERTIFICATE (OPTIONAL).....	52
7.5	COPY MANAGEMENT BACKUP	52
7.6	EPI AND PLUGIN CONFIGURATION FOR TRACING.....	54
7.6.1	EPI Configuration	54
7.6.2	Configuring Plugins	55
7.7	CONFIGURE HTTPS CERTIFICATE ON ODA (OPTIONAL)	60

7.8	CONFIGURE MAIL SERVER (OPTIONAL)	61
7.9	CONFIGURE AUTHENTICATED MAIL SERVER (OPTIONAL)	61
7.10	CONFIGURE SNMP MANAGEMENT SERVER (OPTIONAL).....	62
7.11	MODIFY WEBLOGIC ADMINISTRATION PASSWORD (OPTIONAL).....	62
7.12	MODIFY ORACLE VM IP (OPTIONAL)	62
7.13	CONFIGURE SESSION TIMEOUT (OPTIONAL)	63
7.14	CONTROL HTTPS ACCESS OF MANAGEMENT SERVER ON ODA (OPTIONAL)	63
7.15	CONFIGURE EXTERNAL LDAP (OPTIONAL)	64
7.16	CONTROL CISCO PMP (OPTIONAL)	64
7.17	CONFIGURE THE DEFAULT SETTINGS FOR THE NEW USERS (OPTIONAL)	65
7.18	CONFIGURE CSV STREAMING FEED FEATURE (OPTIONAL).....	65
7.19	CONFIGURE FSE AUTOMATED UPDATE (OPTIONAL)	65
7.20	CONFIGURE NSP FTP OR SFTP SERVER	66
7.21	MANAGEMENT SERVER ONE BOX INSTALLATION ON HP	66
7.22	WEBLOGIC CONSOLE ACCESS ON HTTPS ON ODA(OPTIONAL)	66
8	ACQUISITION MAINTENANCE PROCEDURES	68
8.1	PROCEDURE TO ENABLE/DISABLE TIMESTAMP RESOLUTION TO NANoseconds	68
8.2	FALCO FIRMWARE UPGRADE PROCEDURE.....	68
8.3	KEY EXCHANGE PROCEDURE WITH NEPTUNE PROBE.....	68
8.4	ADD NEW SERVER IN THE INTEGRATED ACQUISITION SUB-SYSTEM	69
8.5	CHANGE THE HOSTNAME OF THE PROBED ACQUISITION SERVER	70
9	MEDIATION MAINTENANCE PROCEDURES	72
9.1	OFFLOAD DFPs FROM THE MEDIATION SERVER	72
9.2	CONFIGURE PDU STORAGE PARAMETERS	73
9.3	ENABLE/DISABLE WRITE ACCESS TO THE PDU MOUNTS.....	74
9.4	SET BEHAVIOR MODE FOR DWS SERVER.....	74
9.5	RE-SYNC THE MEDIATION CONFIGURATION.....	75
9.6	ADD SERVER TO THE MEDIATION SUBSYSTEM.....	75
9.7	ADD MEDIATION SERVER TO THE MEDIATION SUBSYSTEM IN MANAGEMENT/CCM	77
9.8	REMOVE SERVER FROM THE MEDIATION SUBSYSTEM.....	78
9.9	CHANGE MEDIATION NETWORK INTERFACE TYPE TO BONDING	79
9.10	INSTALLATION OF EXTERNAL DATAWAREHOUSE.....	79
9.11	SETUP NFS MOUNT FOR DATAFEED APPLICATION ON CUSTOMER PROVIDED SERVER	82
9.12	EXTERNAL STORAGE CONFIGURATION USING NFS ON ODA	83
9.13	MEDIATION SERVER INSTALLATION ON BLADES	84
9.14	DR STORAGE INSTALLATION ON HP	84
9.15	DATA RECORD STORAGE POST-INTEGRATION CONFIGURATION (OPTIONAL)	84
9.15.1	<i>Activate Session Compression</i>	<i>84</i>
9.15.2	<i>Change Default Passwords of Oracle Accounts (optional)</i>	<i>85</i>
10	PLATFORM BASED MAINTENANCE PROCEDURES	86
10.1	PM&C DISASTER RECOVERY	86
10.2	INSTALL OPERATING SYSTEM ON G6 RACKMOUNT SERVERS	86
10.3	INSTALL OPERATING SYSTEM ON GEN8 RACKMOUNT SERVERS.....	86
10.4	INSTALL OPERATING SYSTEM ON E5-APP-B SERVERS	86
10.5	IPM BLADE SERVERS USING PM&C APPLICATION	86
10.6	SWITCH DISASTER RECOVERY	87

11	EXTERNAL SOFTWARE CONFIGURATION	87
11.1	JAVA RUNTIME SETTINGS	87
11.2	IE BROWSER SETTINGS.....	87
12	KNOWLEDGE BASE PROCEDURES	91
12.1	HOW TO MOUNT THE ISO FILE VIA ILO	91
12.2	CONFIGURE AND VERIFY ILO CONNECTION	91
12.3	ADDING ISO IMAGES TO THE PM&C IMAGE REPOSITORY.....	92
12.4	HOW TO REMOVE IP ADDRESS AND ROUTE	94
12.5	HOW TO RECOVER OA BOARD PASSWORD	94
12.6	GRANTING AND REVOKING DBA ROLE TO NSP USER	95
12.6.1	<i>Revoke DBA role from NSP user after successful NSP installation on one box or oracle box (in case of four box system).....</i>	<i>95</i>
12.6.2	<i>Grant DBA role to NSP user after NSP is installed on one box or oracle box (in case of four box system). 95</i>	
APPENDIXA.	MY ORACLE SUPPORT (MOS)	97
APPENDIXB.	LOCATE PRODUCT DOCUMENTATION ON THE ORACLE TECHNOLOGY NETWORK SITE	98

1 Introduction

1.1 Documentation Admonishments

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

Table 1: Admonishments

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

1.2 Reference Documents

- [1] [Platform 7.0 Configuration Procedure References](#), E53486, December 2014
- [2] [TPD Initial Product Manufacturing](#), E53017, December 2014
- [3] [PIC 10.1.0 Installation Document](#), E53508
- [4] [PIC 10.1.5 Installation document](#), E56065
- [5] [PIC 10.1.5 Upgrade document](#), E56064
- [6] [PM&C Disaster Recovery](#), E54388-02 Release 5.7 and 6.0, November 2014
- [7] [OTD Administration Guide](#), E23389_01
- [8] [ODA Getting Started Guide](#), E22692-41, February 2015
- [9] [Weblogic On ODA](#), E52728, May 2014
- [10] Teklec Default Passwords TR006061
- [11] [PIC Hardware installation Guidelines](#), E64544

1.3 Related Publications

For information about additional publications that are related to this document, refer to the Release Notice document. The Release Notice document is published as a part of the Release Documentation.

1.4 *Scope and Audience*

This document describes the procedures to maintain PIC system at Release 10.1.5. This document covers disaster recovery procedures, IP change procedures as well as various application specific procedures.

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

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

Note: The procedures in this document are not necessarily in a sequential order. There are flow diagrams and high-level overview procedures chapter that provide the sequence of the procedures for each component of this PIC system. Each procedure describes a discrete action. It is expected that the individuals responsible for maintenance of the PIC system should reference these flow diagrams and high-level overview procedures during this process

1.5 *Requirements and Prerequisites*

1.5.1 Hardware Requirements

Refer [PIC Hardware Guidelines](#)

1.5.2 Software Requirements

The following software is required for the PIC 10.1.5 installation.

Oracle Communication GBU deliverables:

- Management Server
- Mediation Server
- Mediation Protocol
- Acquisition Server
- TADAPT
- TPD
- JAVA
 - jdk-7u76-linux-x64.gz
- Oracle WebLogic Server 11gR1 (10.3.6) Generic and CoherenceWebLogic 10.3.6.0
 - wls1036_generic.jarwls1036_generic.jar
- Oracle Database 11.2.0.4 64bits product patchset
 - p13390677_112040_Linux-x86-64_1of7.zip
 - p13390677_112040_Linux-x86-64_2of7.zip
 - p13390677_112040_Linux-x86-64_3of7.zip

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

<https://edelivery.oracle.com/>

On ODA, only the Oracle 11G and Weblogic 10.3.6 is supported. The product files corresponding to 11G and Weblogic 10.3.6 must be downloaded and used in the installation. The patch set files are already mentioned in the ODA documentation(s) [8] and [9]

The latest patch are listed on [Oracle Support Document 1989320.2 \(Information Center: Patches for Oracle Communications Performance Intelligence Center\)](#) and are available at My Oracle Support (MOS)

2 Disaster Recovery Procedures on ODA/ZFS

2.1 DR of Management Server(with DWS database)

Warning: The validity of the backup must be ensured. Please follow section 4.4 in [5]

2.1.1 Management Server Database recreation

The given procedure should be executed in case the management server database on ODA suffered disaster and become non functional, but the oda_base server itself is working fine. In this case it will be sufficient to re-create the management server database using oakcli command after clean up of previous database.

Note: This procedure normally should not impact the DWS database if present on the same ODA.

Use the latest PIC nightly backup to restore the database of Management Server. Make sure the backup is safely kept at external server using either NFS or SFTP.

- a) Log on to Admin Server of Management Server using root and execute below command

```
# service nspservice stop
```

- b) Drop the database by using following steps.

Database should be up before deleting.

1. Log on to oracle box using root user and execute below commands

```
# oakcli show databases
# oakcli delete database -db <db_name>
# oakcli delete dbhome -oh <oracle_home>
```

Where <db_name> is the NSP and <oracle_home> is oracle home for NSP database.

Note: The deletion of database will require multiple times oracle user password.

- c) Refer section **4.3.2 Creation of Management Server database using oakcli** from E56065 Performance Intelligence Center Installation Guide
- d) Refer section **4.5 Management Server user and Tablespace creation** from E56065 Performance Intelligence Center Installation Guide. You can use password as 'nsp' when it prompts to avoid step f.
- e) Refer section **6.1.6 Change nsp user password in database** from E56065 Performance Intelligence Center Installation Guide.
- f) Switch user to oracle on the oracle box and execute below commands:

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

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

The script has four parameters:

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

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

In case restore returns any error, do not proceed ahead and contact Oracle Support [AppendixA. My Oracle Support \(MOS\)](#)

- h) Log in as root on Admin Server and launch the command:

```
# service nspservice start
```

In case service does not start, there could be possibility of wls_internal_ds got corrupted and not working.
This can be recreated only by doing the DR of the weblogic VMs. Perform section 2.1.2 for Weblogic VM DR

2.1.2 Weblogic VMs re-deployment

Note: This procedure normally should not impact the DWS database if present on the same ODA.

The given procedure should be executed in case the disaster occurred for the user VMs (weblogic VMs). It may be possible that file system corruption results in ODA repository not being accessible, which can make VMs non functional. The disaster recovery can be performed to re-deploy the weblogic VMs after proper cleanup.

- a) Clean Weblogic VMs

Log on to ODA_BASE using root user to clean the Weblogic VMs

```
# cd <path of WLS configurator>
# ./cleanup.sh <domain name>
```

Where <domain name> is tekelec for Management Server.

- b) Change nsp user password in database.

1. Log on to oracle box using root user.

2. Change user to oracle and connect as sysdba by executing below commands.

```
# su - oracle
# export ORACLE_SID=NSP
# ORAENV_ASK=NO source oraenv
# sqlplus / as sysdba
```

3. Change password for nsp user

```
# alter user nsp identified by XXXXXXXX;
# quit
```

Password for nsp user can be “default password used for root user”.

- c) Refer section **4.6 Create Weblogic VMs** from E56065 Performance Intelligence Center Installation Guide.

- d) Prepare server for recovery

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

Open a terminal window and log in to Management Admin server as root

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

- e) Refer section from **6 Management Server Application Installation Procedures on ODA** till **6.3.7 Change Customer Icon (Optional)** from E56065 Performance Intelligence Center Installation Guide

- f) Restore realm using below steps

1. Copy PIC backup from external server either by using NFS or SFTP in /opt/oracle/backup on ODA_BASE server.

Note: The ownership of the PIC backup must be **oracle:oinstall** if not then change the ownership to oracle:oinstall using “chown -R oracle:oinstall /opt/oracle/backup/NSP_XXX”

2. [3.9Restore Realm Backup](#)

- g) Log in to Admin server and Run the install script **for builders**

As root, run:

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

Note: Use the same builder ISO which was used before DR.

- h) Perform procedures as mentioned in section 6.3.10 and 6.3.11 in [4] [PIC 10.1.5 Installation document](#), and optional procedures in section 7.7 to 7.10 in current document.

2.1.3 ODA_BASE redeployment

Warning: In this case data of Mediation server will be lost if ODA is shared with management server but Management Server configuration data can be restored by using latest PIC backup if stored on external server.

The below procedure should be executed when the ODA_BASE VM is no more accessible. The dom1 on any of the nodes on ODA is crashed or become non functional.

Use the latest PIC nightly backup to restore the database of Management Server. Make sure the backup is safely kept at external server using either NFS or SFTP.

- a) Refer section **4.2 ODA_BASE Template Deployment** from E56065 Performance Intelligence Center Installation Guide
- b) Refer section **4.3.2 Creation of Management Server database using oakcli** from E56065 Performance Intelligence Center Installation Guide
- c) Refer section **4.5 Management Server user and Tablespace creation** from E56065 Performance Intelligence Center Installation Guide
- d) Refer section **4.6 Create Weblogic VMs** from E56065 Performance Intelligence Center Installation Guide.
- e) Refer section from **6 Management Server Application Installation Procedures on ODA till 6.3.7 Change Customer Icon (Optional)** from E56065 Performance Intelligence Center Installation Guide. **Do not execute** 6.3.6 Schedule Management database backup job on oracle server PIC Global backup after MGMT server installation.
- f) Restore **Database and realm** from backup using below steps
 1. Copy PIC backup from external server either by using NFS or SFTP in /opt/oracle/backup on ODA_BASE server.

Note: The ownership of the PIC backup must be **oracle:oinstall** if not then change the ownership to oracle:oinstall using “chown -R oracle:oinstall /opt/oracle/backup/NSP_XXX”
 2. As root, Execute below command to database and realm restoration

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

In case script returns any error, do not proceed ahead and contact Oracle Support [AppendixA. My Oracle Support \(MOS\)](#)

- g) Perform section 6.3.6 Schedule Management database backup job on Oracle Server from [4] [PIC 10.1.5 Installation document](#),

Note

```
The script nsp_backup_job.sh should end in following lines:  
PL/SQL procedure successfully completed.  
PL/SQL procedure successfully completed.  
PL/SQL procedure successfully completed.
```

- h) Perform procedures as mentioned in section 6.3.10 and 6.3.11 in [4] [PIC 10.1.5 Installation document](#), and optional procedures in section 7.7 to 7.10 in current document.

2.1.4 ODA Physical Server Disaster

Warning: In this case data of Mediation server will be lost if ODA is shared with management server but Management Server configuration data can be restored by using latest PIC backup if stored on external server.

The procedure should be executed in case one or both the physical servers in ODA suffered disaster.

Use the latest PIC nightly backup to restore the database of Management Server. Make sure the backup is safely kept at external server using either NFS or SFTP.

- a) OS installation on both ODA nodes using chapter 4.1 OS Installation in [\[4\] PIC 10.1.5 Installation document](#),
- b) Configure network on ODA, using Chapter 4.1.1 Configure Network in [\[4\] PIC 10.1.5 Installation document](#),
- c) Follow Section [2.1.3 ODA_BASE redeployment](#) in current document to complete the recovery.

2.2 DR of single DWS or multiple DWS(no management server database)

2.2.1 ODA Physical Server Disaster

The procedure is executed if the physical server on ODA becomes non functional because of hardware failure. This is essentially a re-installation of the ODA setup, and creating all the previously hosted database.

Warning: Data will be lost.

1. Set the DWS in maintenance mode by using [9.4 Set Behavior Mode for DWS Server](#)
2. Refer to **Installation document [4]** ,
 - a. Perform steps in section **4.1 for OS installation**,
 - b. Perform steps in section **4.2 for ODA_BASE deployment**
 - c. Perform steps in **4.3.1 for Creation of DWS database**
 - d. Perform steps in **4.4 for creation of user and tablespaces**.
 - e. Perform steps in **section 8.1 and 8.2**

Note: If the ODA was hosting multiple DWS database, then step 4.3.1 and 4.4 should be repeated for all the database.

3. If the DWS was **active** before the DR, reset it to active mode using [9.4 Set Behavior Mode for DWS Server](#)

2.2.2 ODA_BASE Disaster

The procedure is executed if the (ODA_BASE) dom1 virtual machine becomes non functional. This is essentially a re-deployment of the ODA_BASE server, and creating all the previously hosted database.

Warning: Data will be lost.

1. Set the DWS in maintenance mode by using [9.4 Set Behavior Mode for DWS Server](#)
2. Refer to **Installation document [4]** ,
 - a. Perform steps in section **4.2 for ODA_BASE deployment**
 - b. Perform steps in **4.3.1 for Creation of DWS database**

- c. Perform steps in **4.4 for creation of user and tablespaces.**
- d. Perform steps in **section 8.1 and 8.2**

Note: If the ODA was hosting multiple DWS database, then step 4.3.1 and 4.4 should be repeated for all the database.

3. If the DWS was **active** before the DR, reset it to active mode using [9.4 Set Behavior Mode for DWS Server](#)

2.2.3 DWS database re-creation

The given procedure should be executed in case the particular DWS database on ODA suffered disaster and become non functional, but the oda_base server itself is working fine. In this case it will be sufficient to re-create the DWS database using oakcli command after clean up of previous database.

Note: This procedure normally should not impact the other DWS databases if present on the same ODA.

1. Set the DWS in maintenance mode by using [9.4 Set Behavior Mode for DWS Server](#)
2. Drop the database by using following steps.
Database should be up before deleting.

- a. **Log on to oracle box using root user and execute below commands**

```
# oakcli show databases
# oakcli delete database -db <db_name>
# oakcli delete dbhome -oh <oracle_home>
```

Where <db_name> is the DWS database name and <oracle_home> is oracle home for DWS database.

Note : The deletion of database will require multiple times oracle user password

3. Perform steps in **4.3.1 for Creation of DWS database** in [\[4\]](#)
4. Perform steps in **4.4 for creation of user and tablespaces** in [\[4\]](#)
5. **Perform steps in section 8.1 and 8.2** in [\[4\]](#)
6. If the DWS was **active** before the DR, reset it to active mode using [9.4 Set Behavior Mode for DWS Server](#)

Note: lxpStore process on the mediation server may need to be restarted, after the above procedures are completed.

2.3 DR of single DWS(with Management Server database)

Warning: Re-installing ODA_BASE or ODA can result it management server re-installation in case the ODA is shared between DWS and management server.

2.3.1 ODA Physical Server Disaster

One or both physical server in ODA failed and this requires the re-installation of the ODA setup. However if the DWS is sharing the management database also, then configuration can be restored using the nightly backup, if already stored on the external backup.

Warning: Only management database configuration can be restored, the data stored in DWS will be lost.

The DR will require management server re-installation along with DWS re-installation and following steps should be performed:

1. Perform **4.1 OS installation** from [\[4\] PIC 10.1.5 Installation document](#),
2. Perform steps in section **4.2** for ODA_BASE deployment in [\[4\] PIC 10.1.5 Installation document](#),
3. Perform steps in **4.3.1** for Creation of DWS database in [\[4\] PIC 10.1.5 Installation document](#),
4. Perform steps in **4.4** for creation of user and tablespaces in [\[4\] PIC 10.1.5 Installation document](#),

5. Perform steps in **section 8.1 and 8.2** in [4]
6. Perform steps from **step b)** onwards from section Section 2.1.3 ODA_BASE redeployment in current document to complete the recovery.

2.3.2 ODA_BASE Disaster

The below procedure should be executed when the ODA_BASE VM is no more accessible. The dom1 on any of the nodes on ODA is crashed or become non functional. However if the DWS is sharing the management database also, then configuration can be restored using the nightly backup, if already stored on the external backup.

Warning: Only management database configuration can be restored, the data stored in DWS will be lost.

1. Perform steps in section 4.2 for ODA_BASE deployment in [4] PIC 10.1.5 Installation document,
2. Perform steps in 4.3.1 for Creation of DWS database in [4] PIC 10.1.5 Installation document,
3. Perform steps in 4.4 for creation of user and tablespaces in [4] PIC 10.1.5 Installation document,
4. Perform steps in **section 8.1 and 8.2** in [4]
5. Perform steps from **step b)** onwards from section Section 2.1.3 ODA_BASE redeployment in current document to complete the recovery.

2.3.3 DWS database re-creation

Note: This will not have impact on the management server running on ODA.

Refer Section 2.2.3 DWS database re-creation

2.4 DR of ZFS

PIC does not support disaster recovery on ZFS server. In case of disaster e.g. hardware failure, disk failure on ZFS storage appliance following documentation can be referred:

- ZFS storage appliance administration guide, https://docs.oracle.com/cd/E56021_01/pdf/E55851.pdf
- Chapter 11 in ZFS administration guide, <http://docs.oracle.com/cd/E19253-01/819-5461/>

1. Disconnect the PDU directories shared by the ZFS

As root, on each server of the subsystem, run:

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit
```

On one server of the subsystem, as root, backup the bulkconfig file:

```
# cp /root/bulkconfig /root/bulkconfig.bak
```

Then, edit the bulkconfig file. Locate the lines starting with the pdu keyword, followed by the IP of the ZFS, and remove them. As root, adjust the subsystem PDU settings with the following command:

```
# bc_adjust_subsystem.sh
```

2. DR the ZFS (refer to the documentation listed here above)

3. Reconnect the PDU directories shared by the ZFS

On the server of the subsystem, where the bulkconfig file has been backed up, as root, run:

```
# mv -f /root/bulkconfig.bak /root/bulkconfig
```

As root, adjust the subsystem PDU settings with the following command:

```
# bc_adjust_subsystem.sh
```

As root, on each server of the subsystem, run:

```
# /usr/TKLC/plat/sbin/rootSshLogin --revoke
```


3 Management Server Disaster Recovery Procedures

3.1 Management Server One-Box HP

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

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

4. Reinstall Operating System on the management server

Estimation: 30 min

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

Install the operating system following right procedure:
Refer [Server IPM](#) for IPM instructions.

5. Resize /var/TKLC/partition

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

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

6. Mount oracle volume

Estimation: 10 min

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

7. Management Server one box fresh install

Estimation: 70 min

Complete installation by following the steps:

1. [NSP Pre-Install Configuration](#)
2. [Install WebLogic](#)

3. [Install Oracle Database](#)
4. [Install NSP](#)
5. The nightly backup folder NSP_BACKUP contains the optional_modules_list file. This file should be referred to install optional applications that were present before disaster recovery procedure. Install only those optional modules from post installation procedure that are present in this file.

8. Check permission for backup directory

Execute following commands as root:

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

Where nsp_bakckup_timestamp refers to the backup directories created nightly

NOTE: Management Server creates two different types of backups:



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

9. Restore the database and realm

Following the steps:

- a. [Restore Realm Backup](#)
- b. [Recover NSP Database on One-Box setup](#)

10. Reboot the server

11. Log in on the server and Run the install script for builders

As root, run:

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

Note: Use the same builder ISO which was used before DR.

12. Set Global Names to false

```
# su - oracle
# sqlplus / as sysdba
# ALTER SYSTEM SET GLOBAL_NAMES=FALSE;
```

13. Perform NSP Post-Install Sanity Check

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

3.2 management Server Four-Box on HP



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

The servers must be backout in the order described below:

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

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

3.2.1 Apache Server (Four-Box)

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

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

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

1. Reinstall Operating System on the Management server

Estimation: 30 min

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

Install the operating system following right procedure:

Refer [Server IPM](#) for IPM instructions

2. Resize /var/TKLC/partition

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

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

3. Complete the Management Apache installation

Complete installation by following the steps:

1. [NSP Pre-Install Configuration](#)
2. [Install NSP](#)

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

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

3.2.2 Oracle Server (Four-Box)

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

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

1. Reinstall Operating System on the Management Server server

Estimation: 30 min

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

Install the operating system following right procedure:

Refer [Server IPM](#) for IPM instructions

2. Resize /var/TKLC/partition

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

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

3. Mount oracle volume

Estimation: 10 min

- For C-class blade setup follows Remount Management Server LUN(C-class blades only)
- For Rackmount servers follows [Mount oracle volume \(Rackmount only\)](#)

4. Install the oracle server

Complete installation by following the steps:

1. [NSP Pre-Install Configuration](#)
2. [Install Oracle Database](#)
3. [Install NSP](#)

5. Check permission for backup directory

Execute following commands as root:

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

Where nsp_backup_timestamp refers to the backup directories created nightly

NOTE: Management Server creates two different types of backups:



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

6. Restore the oracle database

Following the steps: Recover Management Server Database on Four-Box setup

7. Reboot the Management Server Oracle server

8. Set Global Names to false

```
# su - oracle
# sqlplus / as sysdba
# ALTER SYSTEM SET GLOBAL_NAMES=FALSE;
```

9. Perform Management Server Post-Install Sanity Check

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

3.2.3 Secondary WebLogic (Four-Box)

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

1. Reinstall Operating System on the Management Server server

Estimation: 30 min

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

Install the operating system following right procedure:

Refer [Server IPM](#) for IPM instructions

2. Resize /var/TKLC/partition

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

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

3. Complete the Management Server Secondary WebLogic Installation

Complete installation by following the steps:

- [NSP Pre-Install Configuration](#)
- [Install WebLogic](#)
- [Install NSP](#)

4. Recover the Primary server

Following the steps: [Primary WebLogic \(Four-Box\)](#)

5. Reboot the Management Server Secondary server

6. Perform Management Server Post-Install Sanity Check

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

3.2.4 Primary WebLogic (Four-Box)

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

1. Reinstall Operating System on the Management Server server

Estimation: 30 min

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

Install the operating system following right procedure:

Refer [Server IPM](#) for IPM instructions

2. Resize /var/TKLC/partition

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

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

3. Prepare server for recovery

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

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

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

4. Restore optional modules files

Copy the optional modules list file from backup into /tmp

As root run:

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

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

5. Complete the Management Server Primary WebLogic Installation

Complete installation by following the steps:

1. [NSP Pre-Install Configuration](#)
2. [Install WebLogic](#)
3. [Install NSP](#)

6. Import the Realm

Following the steps: [Restore Realm Backup](#)

7. Reboot all the Management Server cluster

Reboot all 4 Management Server servers from the Four-Box setup:

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

8. Restore SNMP and SMTP configuration

- a. For SNMP, follow the Modify SNMP Agent IP Address procedure in [PIC10.1.0 Installation Guide](#)
- b. For SMTP, follow the Configure Mail Server procedure in [PIC10.1.0 Installation Guide](#)

9. Log in on the server and Run the install script for builders

As root, run:

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

Note: Use the same builder ISO which was used before DR.

10. Perform Management Server Post-Install Sanity Check

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

3.3 Mount oracle volume (Rackmount only)

Run this procedure as root:

1. Mount Management Server ISO

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

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

2. Mount oracle volume

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

3. Umount ISO

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

3.4 Remount Management Server LUN(C-class blades only)

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

Prerequisite:

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

1. Login as root user on the Management Server server for onebox setup or oracle server of a four box Management Server (all following commands are executed as root)

2. Retrieve LUN numbers of logical volumes

```
# multipath -ll
```

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

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

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

- Lun# for REDO is the one in the block containing [size=70G] (37 for mpath0 in example)
- Lun# for DATA is the one in the block containing [size=419G](36 for mpath1 in example)
- Lun# for BACKUP is the one in the block containing [size=139G](35 mpath2 in example)

3. Recreate mapping to SAN REDO volume

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

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

- b. When prompted for **Login on Remote** with the user `platcfg`
c. After completion, the output must show:

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

4. Recreate mapping to SAN DATA volume

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

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

- b. When prompted for **Login on Remote** with the user `platcfg`
c. After completion, the output must show:

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

5. Recreate mapping to SAN BACKUP volume

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

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

- b. When prompted for **Login on Remote** with the user `platcfg`
c. After completion, the output must show:

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

6. Check the volume names

```
# multipath -ll
```

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

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

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

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

It should no longer show mpath0, mpath1 and mpath2.

7. Check the file system

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

8. Mount the volumes

```
# mount -a
```

9. Verify the volumes

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

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

3.5 Management Server Pre-Install Configuration

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

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

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

- Configure the Management Server server hostname.
Note: This configuration is required to get the hardware alarms forwarded by the system as SNMP traps into Management Server ProAlarm.
- Configure SNMP.
- Add cdrom entry to /etc/fstab.
Note: The purpose of adding this entry is to simplify mount commands that will be used throughout the Management Server installation process.

Before you perform this procedure, make sure you have read and are familiar with the “**PIC bulkconfig file description**” in [PIC 10.1.5 Installation Guide](#). This procedure must be performed on each Management Server server (single server for a one-box; all four servers for a four-box).

1. Login as root user on the Management Server server for onebox setup or oracle server of a four box Management Server (all following commands are executed as root)
2. On each HP based management server permit root ssh login.

a) As root run:

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit
```

3. Check system health

```
# syscheck
```

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

Example output for a healthy system:

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

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

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

a. Enter the **platcfg**

```
# su - platcfg
```

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

6. Configure SNMP

- a) From the main platcfg menu, select Network Configuration > SNMP Configuration > NMS
- b) Configuration and select Edit > Add A New NMS Server.
- c) Enter
Hostname or IP: 127.0.0.1

Port: 162
SNMP Community String: TEKELEC
and then click OK and then EXIT

- d) Click YES to restart alarm server and then press any Key to continue.
- e) Exit the platcfg menu.

3.6 Install WebLogic

This procedure describes how to install the WebLogic software for the Management Server (single server for a One-box; On the designated Primary and Secondary WebLogic servers for a Four-box). Before you perform this procedure:

- Make sure that you have the WebLogic files available. Copy all the weblogic product file `wls1036_generic.jar` and latest JDK 7 file indicated in section [1.5.2 Software Requirements](#) to `/var/TKLC/upgrade` directory on the server.
- Verify the `/root/bulkconfig` file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.

Note: Run this procedure via ILO.

3.6.1 Mount Management Server media

As root, run:

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

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

3.6.2 Install WebLogic Product

As root, run:

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

Wait until the installation process is complete.

Analyze the installation log

Verify that WebLogic installed successfully.

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

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

If this message does not appear in the log file, contact the Oracle [My Oracle Support \(MOS\)](#).

3.7 Install Oracle Database

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

Before you perform this procedure:

- Make sure that you have the Oracle files available. Copy all the Oracle product files indicated in section [1.5.2 Software Requirements](#) to `/var/TKLC/upgrade` directory on the server.
- Verify the `/root/bulkconfig` file needed for this installation has been created on the server accordingly to specific application directions as a result of pre-install configuration step.
- In case of c-class blades SAN Configuration must be done properly before starting Oracle Installation

Note: Run this procedure via ILO.

As root, run:

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

Wait until the installation process is complete.

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

Analyze the installation log:

Verify that Oracle installed successfully.

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

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

If this message does not appear in the log file, contact the [My Oracle Support \(MOS\)](#).

3.8 Install Management Server

3.8.1 Mount Management Server media

As root, run:

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

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

3.8.2 Install Management Server application

As root, run:

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

Wait until the installation process is complete.

Analyze the installation log:

Verify that Management Server installed successfully.

After the installation the server will restarts automatically. Log back in and review the Management Server

installation log (/var/log/nsp/install/nsp_install.log) and TPD upgrade log

(/var/TKLC/log/upgrade/upgrade.log) for errors.

If Management Server did not install successfully, contact the Oracle Support.

Note: When user will login back to machine then a message will appear asking to accept or reject upgrade. Ignore this message for now. It will be automatically accepted when user will execute

post_upgrade_sanity_check.sh script during [3.11 Management Server Post-Install Sanity Check \(onebox and four box\)](#)

3.9 Restore Realm Backup

This procedure describes how to restore the Management Server realm backup.

NOTE: During Disaster recovery the Nightly Backup present at /opt/oracle/backup/ folder with names NSP_BACKUP_dd_mm_yy_hh_mm_ss must be used

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

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

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

OR

In case of ODA copy the realm backup into a local directory of AdminServer:

```
# scp -r oracle_ip_address:/opt/oracle/backup/nsp_backup_dir/ /opt/nsp/
```

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

3. Execute the following commands:

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

Note: Make sure the backup directory is owned by tekelec user. If not change ownership to tekelec before running command below

In case of HP

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

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

Or in case of ODA

```
#source /opt/nsp/scripts/procs/nsp_setenv.sh
#export NSP_PKG_DIR=/opt/nsp/nsp-package
# cp $NSP_PKG_DIR/framework/server/dist/server/importRealm.py
$NSP_PKG_DIR/framework/server/dist/server/importRealm.py_bkup
#sed -i "s/t3:\\/\\/t3:\\/\\/$NSP_J2EE_HOST/g;s/+adminServerListenAddress//g"
$NSP_PKG_DIR/framework/server/dist/server/importRealm.py
#sh /opt/nsp/scripts/LaunchImpNSPrealm.sh backup_dir
# cp $NSP_PKG_DIR/framework/server/dist/server/importRealm.py_bkup
$NSP_PKG_DIR/framework/server/dist/server/importRealm.py
```

Note: Enter Yes when prompted for replacing the file during file copy.

Where backup_dir is the directory which contains the backup of realm data (e.g. /opt/nsp/NSP_BACKUP_10_14_10_22_00_01/)

3.10 Recover Database

3.10.1 Recover Management Server Database on One-Box setup or ODA

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

1. Prerequisites for using Import Utility to Restore a Database

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

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

- Prerequisite for restoring a database

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

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

Otherwise use the following command to set write permission:

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

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

As root user go to folder <DIR_CONTAINING_DUMP>:

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

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

2. Import utility

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

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

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

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

a) Log in as root on Management Server (One-box) and launch the command:

```
# service nspservice stop
```

b) Login as root user on Management Server Server for one-box and launch the command:

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

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

The script has four parameters:

- Oracle connection string (NSP/NSP) must not be modified
- Name of the exported schema name (NSP) must not be modified

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

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

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

```
# service nspservice start
```

3.10.2 Recover Management Server Database on Four-Box setup

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

1. Prerequisites for using Import Utility to Restore a Database

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

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

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

- Prerequisite for restoring a database

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

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

Otherwise use the following command to set write permission:

- a. Login as `root` on Management Server Oracle (Four-Box).

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

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

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

As `root` user go to folder `<DIR_CONTAINING_DUMP>`:

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

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

2. Stop WebLogic

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

```
# service nspservice stop
```

3. Restore the Management Server database

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

- a. Login as root on Management Server Oracle (Four-Box).
- b. The following command restores the Management Server database after stopping the Oracle listener. After the restore is complete the Oracle listener is restarted. As root run:

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

The script has four parameters

- Oracle connection string (NSP/NSP) must not be modified
 - Name of the exported schema name (NSP) must not be modified
 - Target schema name (NSP) must not be modified
 - The backup_dir is the path of the directory which contains the exported database file(**ExpNSP.dmp.gz**).
- Ex: backup dir = /opt/oracle/backup/NSP_BACKUP_06_12_12_22_00_01/oracle

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

4. Restart weblogic

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

```
# service nspservice start
```

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

Login as tekelec user on Management Server Server

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

Switch to root user and run:

```
# service nspservice restart
```

3.11 Management Server Post-Install Sanity Check (onebox and four box)

Box: Onebox/Four Box

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

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

Note: When user will execute this script it will automatically accept the upgrade. However during this step the server will be rebooted. The logs should be verified after the server has come up from reboot.

3. Review the Management Server installation logs (/var/log/nsp/install/nsp_install.log).
4. Verify the following:
 - Port 80 connectivity is OK
 - Oracle server health is OK
 - WebLogic health for ports 5556, 7001, 8001 is OK
 - Oracle em console connectivity is OK
 - The disk partition includes the following lines, depending on whether rackmount or blades setup:
 - If rackmount, the output contains the following lines:

```
/dev/sdc1      275G 4.2G 271G  2% /usr/TKLC/oracle/ctrl1
/dev/sdb1      825G 8.6G 817G  2% /usr/TKLC/oracle/oradata
/dev/sdd1      275G 192M 275G  1% /usr/TKLC/oracle/backup
```

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

- If blades, output contains following lines:

```
/dev/mapper/nsp_redo_vol 69G 4.2G 61G 7% /usr/TKLC/oracle/ctrl1
/dev/mapper/nsp_data_vol 413G 76G 316G 20% /usr/TKLC/oracle/oradata
/dev/mapper/nsp_backup_vol 138G 9.2G 121G 8% /usr/TKLC/oracle/backup
```

5. On each HP based management server revoke root ssh login.

- a) As root run:

```
# /usr/TKLC/plat/sbin/rootSshLogin --revoke
```

4 Acquisition Disaster Recovery Procedures

4.1 Acquisition Server Disaster Recovery

1. Reinstall Operating System

Install the operating system following right procedure:

Refer [2] [TPD Initial Product Manufacturing, E53017, December 2014](#) for IPM instructions.

2. Install Acquisition Application

Refer [5] [PIC 10.1.5 Upgrade document, Chapter 6](#)

5 Mediation/DWS Disaster Recovery Procedures

Note: It may be require to give root ssh access before executing many procedures. Please give the access and then revoke it after completing the procedures, as mentioned below

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit
```

```
# /usr/TKLC/plat/sbin/rootSshLogin --revoke
```

5.1 Mediation/DWS Disaster Recovery Overview

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

The procedure is applicable to the following server types:

- DWS Server
- Mediation PDU Storage Server
- Mediation Base Server

The procedure is applicable to the following hardware types:

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

Note on DWS: During the disaster recovery procedure of DWS Server you must install the same version of the Oracle database as the current one. However, this procedure only applies to DWS freshly installed as part of PIC 10. Thus, if Oracle 10g is installed, the disaster recovery procedure can not be applied and you have to go for a new installation (refer to the installation document [4] , section INSTALLATION OVERVIEW FOR DWS).

If Oracle 11g is currently installed then the disaster recovery procedure for DWS can be executed. Check the Oracle version on the DWS Server as root with the following command:

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

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

5.1.1 HP DWS server disaster recovery procedure

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

1. **Set the DWS in** maintenance mode, follow [9.4 Set Behavior Mode for DWS Server](#)
2. **Retrieve LUN number for C-class blades only** follow [5.6 Retrieve LUN numbers \(C-class blades only\)](#)
3. **Refer to Installation document [3] [4] , Section DWS Installation Procedures. Note:**
 - bulkconfig file must contain DR-XDR platform function value.
 - **for C-class blades setup**, don't run SAN configuration step but run [5.7 Remount LUN \(C-class blades only\)](#)
 - execute all the other steps until Integration to customer network (this is the last step of the DWS Installation procedure to execute).
4. **If the DWS was active before the DR, reset it in active mode using** [9.4 Set Behavior Mode for DWS Server](#)

5.1.2 Mediation PDU Storage server disaster recovery procedure.

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

1. **Stop IXP service using [5.2 Stop IXP Service](#) (if the server is accessible)**
2. **Disintegrate Server with Mediation Subsystem [5.3 Disintegrate Server with the Mediation Subsystem](#)**
3. **Retrieve LUN Numbers for logical volumes (C-class blades only) using [5.6 Retrieve LUN numbers \(C-class blades only\)](#)**
4. **Refer to Installation document [4] , Section IXP Installation Procedures. Note:**
 - bulkconfig file must contain DR-PDU platform function value.
 - **for C-class blades setup**, don't run SAN configuration step but run [5.7 Remount LUN \(C-class blades only\)](#)
5. **Integrate Server with in mediation sub-system using [5.4 Integrate Server with the Mediation Subsystem](#)**
6. **Remount Export Directories using [5.5 Remount Export Directories](#)**

5.1.3 Mediation Base server disaster recovery procedure.

Follow the references below in a sequential order to recover Mediation Base server: [5.1.2 Mediation PDU Storage server disaster recovery procedure](#), [IXP PDU Storage](#)

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

5.2 Stop IXP Service

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

Open a terminal as root on the mediation server:

```
# service TKLCixp stop
```

5.3 Disintegrate Server with the Mediation Subsystem

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

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

```
$ analyze_subsystem.sh
```

Analyze the output of the script for errors. Issues reported by this script must be resolved before any further usage of this server. Verify no errors are present (ignore error messages regarding the server that is going to be disintegrated for the subsystem).
If errors occur, contact the Oracle Support, AppendixA. My Oracle Support (MOS)
.
2. **Remove a host record from the bulkconfig file**
 - a) As `root` user, remove a host record with the server you want to disintegrate from the `/root/bulkconfig` file.
 - b) Make sure now the `/root/bulkconfig` file contains all remaining servers in the subsystem with valid parameters.
3. **Update mediation subsystem servers**
 - a) Run the following script to adjust the mediation subsystem network and other settings accordingly to the `/root/bulkconfig` file. As `root` run:

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit  
# bc_adjust_subsystem.sh
```
 - b) Wait until system reconfigures.

- c) Verify that the mediation subsystem has been reconfigured correctly. As `root` run:

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


If any error occurs contact the Oracle Support AppendixA. My Oracle Support (MOS)

5.4 Integrate Server with the Mediation Subsystem

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

1. **Add a host record to the bulkconfig file with the recovered server**
 - a) Open a terminal window and log in to the recovered server as `root` user.
 - b) Recreate the `/root/bulkconfig` file. You can copy the content of the `/root/bulkconfig` from any other server in the mediation subsystem.
 - c) Add a host record for the recovered server with the valid information into the `/root/bulkconfig` file.
 - d) Make sure now the `/root/bulkconfig` file contains all servers in the subsystem with valid parameters.
2. **Restore shared directories and Data Feed status**
 - a) Restore possible shared directories by running, as `root`:

```
# ixp_postinstall_restore.sh
```
 - b) Restore Data Feed status by running, as `root`:

```
# RestoreDataFeedStatus.sh --local
```
3. **Update Mediation subsystem**
Refer to Update mediation subsystem servers.
4. **Copy the xDR Builder rpm if not present**
 - a) Login into Management Server One-box or primary box (in case of four box) as `root` user and execute the below command to check if the xDR builder rpm is present.

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


If the above command shows the xDR builder rpm then do not execute step b).
 - b) Copy the xDR builder rpm to path `/var/TKLC/jmxagent/upload/`
Note: xDR builder rpm which is mentioned in load line up
5. **Install the xDR Builder package**
All servers in the Mediation subsystem must have the same xDR builders package.
As `cfguser` run:

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


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

5.5 Remount Export Directories

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

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

```
$ sudo umount /opt/TKLCdataexport/mount/*
```
3. **DataFeed will mount exporting directories back by itself.**

5.6 Retrieve LUN numbers (C-class blades only)

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

Retrieve volume names and LUN numbers from SAN configuration file

As root run:

```
# multipath -ll
```

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

5.7 Remount LUN (C-class blades only)

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

1. Check the volume are visible from the server.

As root run:

```
# multipath -ll
```

If the command is returning a result you can proceed with the next step; if not try to reboot the server.

2. Remount LUN on DWS

Note: ignore this step for Mediation PDU servers

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

```
# /usr/TKLC/plat/bin/tpdProvd --client --subsystem=TPD::SOAP::Storage  
addVolumeInfo name volume_name lun lun_number fstype raw
```

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

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

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

3. Remount LUN on Mediation PDU servers

Note: ignore this step for DWS

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

```
# /usr/TKLC/plat/bin/tpdProvd --client --subsystem=TPD::SOAP::Storage  
addVolumeInfo name volume_name lun lun_number mount mount_dir
```

where *volume_name* is the name of the volume you have retrieved from SAN template, *lun_number* is corresponding LUN number you have retrieved from SAN template and *mount_dir* depends on what server is being updated:

- o /pdu_1, when remounting the first PDU filesystem LUN of an Mediation PDU server
- o /pdu_2, when remounting the second PDU filesystem LUN of an Mediation PDU server

Note: Provide password for “platcfg” user.

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

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

4. Check the volume names

a) As root run:

```
# multipath -ll
```

b) Example output for xDR Storage Server with file based Oracle 10g. Note that `mpath*` entries are renamed and also mounted and such visible in output of the mount command.

```
1_oracle_data (3600c0ff000d5809fb180cc4901000000) dm-6 HP,MSA2012fc
[size=1.4T][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:0:37 sdc 8:32 [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 1:0:0:37 sdd 8:48 [active][ready]
1_oracle_index (3600c0ff000d579384780cc4901000000) dm-5 HP,MSA2012fc
[size=1.4T][features=0][hwhandler=0]
\_ round-robin 0 [prio=1][active]
\_ 0:0:1:36 sda 8:0 [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 1:0:1:36 sdb 8:16 [active][ready]
```


6 PIC IP Changes Procedure

The PIC IP change procedure are defined for the HP based system which are installed over TPD platform.

6.1 PIC IP Change Overview

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

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

Note: This procedure must be run via ILO

1. **Disable all feeds associated with Mediation subsystems and Export File Server**

Note: Execute this step if you are going to migrate Mediation subsystem or Export File Server.

- a. Open a web browser and log in to Management Server application interface and navigate to **DataFeed** application.
- b. Click on **xDR/KPI Feeds** and deactivate all feeds that are associated with the Export Servers or Mediation subsystems that going to be migrated to new network settings

2. [Management Server IP Change Procedure](#)

3. [Acquisition subsystem IP Change Procedure](#)

4. [Mediation Subsystem IP Change Procedure](#)

5. [DWS IP Change Procedure](#)

6. **Enable all feeds associated with Mediation subsystems and Standalone Export Servers**

Note: Execute for all feeds that has been disactivated before PIC IP change procedure.

- a. Open a web browser and log in to Management Server application interface and navigate to **DataFeed** application.
- b. Click on **xDR/KPI Feeds**
- c. Check feed associated with the affected Export Server(s)
- d. Click on **Modify** icon and navigate to IP address of Export Server. e) Change the IP address and save changes. **Activate** the feed.
- e. Repeate steps c-e for all affected feeds.

6.2 Management IP Change Procedure

Warning: The procedure to change the management server IP address on ODA is not supported. The given procedures are applicable for HP based management server.

This procedure describes the Management Server IP change procedure.

Note: This procedure must be run via ILO

1. **Modify Management Server IP Address:**

- Management Server One-Box:
 - a. [Modify Management One-Box IP Address](#)

- Management Server Four-Boxes:
 - a. [Modify Management Apache IP Address \(Four-Box Configuration\)](#)
 - b. [Modify Management Secondary or Oracle IP Address \(Four-Box Configuration\)](#)
 - c. [Modify Management Primary IP Address \(Four-Box Configuration\)](#)
- 2. [Update Management IP addresses on xMF](#)
- 3. [Update Management IP addresses on IXP or EFS](#)

6.2.1 Modify Management One-Box IP Address

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

Run this procedure as root:

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

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

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

- eth01 for Rackmount
- bond0.3 for blade

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

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

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

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

```
# su - platcfg
```

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

Click Edit.

Click Yes.

The IP address is changed.

Exit the platcfg menu

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

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

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

6.2.2 Modify Management Apache IP Address (Four-Box Configuration)

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

Run this procedure as root:

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

2. Follow Steps 1 to 3 [Modify Management One Box IP address](#)

6.2.3 Modify Management Secondary or Oracle IP Address (Four-Box Configuration)

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

Run this procedure as root:

1. Open a terminal window and log in as `root` on the Management Server Apache server.
2. Follow Steps 1 to 3 [Modify Management One Box IP address](#)

6.2.4 Modify Management Primary IP Address (Four-Box Configuration)

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

Following the step [Modify Management One-Box IP Address](#)

6.2.5 Update Management IP addresses on xMF

This procedure describes the steps to update the Management Server IP addresses on Acquisition subsystems.

Run this procedure as root:

1. Update appservers (nsp primary and nsp secondary) in `/root/bulkconfig` file with appropriate values
2. Run bulkconfig script:

```
# /opt/TKLCmf/bin/bulkConf.pl
```
3. Reboot the server

6.2.6 Update Management IP addresses on IXP or EFS

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

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

Run this procedure as root:

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

```
# bc_adjust_subsystem.sh
```

The IP addresses of Management Server servers will be changed on all servers in the Mediation subsystem or EFS.

6.3 Acquisition subsystem IP Change Procedure

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

Note: This procedure must be run via ILO

6.3.1 Change IP Addresses

Run this procedure as root:

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

```
# /opt/TKLCmf/bin/bulkConf.pl
```
3. Reboot the server

6.3.2 Change VIP Addresses

Note: This is run on the primary server only

1. Login to **primary** server as **cfguser**
2. Run setSSVIP script:
 - If the Acquisition server is standalone Probed server then execute following command:

```
setSSVIP -s
```
 - If the Acquisition server is primary server of integrated acquisition sub-system then execute following command:

```
setSSVIP <VIP>
```

Where <VIP> is VIP address of the acquisition sub-system

6.3.3 Change IP Address Acquisition subsystem in Management

Note: These steps have to be performed on the management server irrespective it is on ODA or HP.

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

6.4 Mediation Subsystem IP Change Procedure

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

Use this procedure in following cases:

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

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

Note: This procedure must be run via ILO

1. Update the bulkconfig file

- a. Login to the iLO as root of any Mediation server in the subsystem you are about to reconfigure
- b. Update the /root/bulkconfig file with the new IP addresses

2. Run IP change procedure

- a. Run the Mediation subsystem IP change procedure as root:

```
# bc_changeip_subsystem.sh
```

- b. The Mediation subsystem healthcheck procedure will be triggered.
- c. If the healthcheck procedure will end with no errors then the script will automatically continue with the IP change procedure. If there will be errors you will be asked for confirmation if you want to continue. You can continue, but on your own risk. There is NO GUARANTEE that the system will be functional after and that the rest of the procedure will pass.
- d. If you migrate the Mediation subsystem in a scope of a single network the script will run until the end and there is no additional operation needed.
- e. Perform any hardware related configuration like cabling etc.
- f. Log in to the server where you have previously updated the bulkconfig file as root and run:

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

Wait until the procedure finishes. Check for any errors. In case of any errors contact the Oracle Support, [AppendixA. My Oracle Support \(MOS\)](#)

Note: These steps mentioned in point 3, 4 and 5 have to be performed on the management server irrespective it is on ODA or HP.

3. Change Mediation subsystem IPs in Management

- a. Login to the Management Server GUI and navigate to **Centralized Configuration** Application
- b. Navigate to **Equipment Registry** in Left Tree Panel
- c. Click on **IXP**  **IXP Subsystem**
- d. Modify the servers and change **Admin IP address** field to the new IP address

4. Change Mediation subsystem's VIP in Management Server

- a. Login to the Management Server GUI and navigate to **Centralized Configuration** Application
- b. Navigate to **Equipment Registry** in Left Tree Panel
- c. Click on **Mediation**
- d. Modify the subsystem and change **VIP Address** field to the new IP address
- e. Click Modify

5. Apply changes

- a. Navigate to the **Mediation** view
- b. Navigate to **Sites**
- c. Open **IXP** and right-click on the subsystem.

- d. Select **Apply changes...** from the popup menu.
- e. Click on the **Next** button
- f. Click on the **Apply Changes** button.
- g. Wait until changes are applied.
- h. Verify that result page does not contain any errors.

6.5 DWS IP Change Procedure

Warning: For ODA based DWS, the IP change procedures are not supported.

This procedure describes how change the IP settings on the DWS. This procedure is applicable only for the HP based DWS server.

Use this procedure in following cases:

- Server IP change
- Netmask change
- Default gateway change

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

Note: This procedure must be run via ILO

1. Update the bulkconfig file

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

2. Run IP change procedure

- a. Run the DWS subsystem IP change procedure as root:

```
# bc_changeip_subsystem.sh --pre
```

- b. Continue with:

```
# bc_changeip_subsystem.sh --change
```

- c. Continue with:

```
# bc_changeip_subsystem.sh --post
```

- d. Finalize the IP change procedure on the DWS, as cfguser:

```
$ makeDWH.sh
```

Confirm, enter passwords where needed.

Note: These steps mentioned in point 3 and 4 have to be performed on the management server irrespective it is on ODA or HP.

3. Change DWS IP in Management Server

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

4. Apply changes

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

7 Management Server Maintenance Procedures

Warning: On ODA, if the management server database has been restarted in any procedure or during some investigation then nspservice must be restarted on the management Admin Server in ODA.

7.1 Management Server Backup Procedures

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

7.1.1 Automatic Backup

7.1.1.1 Activate Automatic Management Server Backup

This procedure describes how to activate the automatic backup procedure.

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

1. Verify if the backup is activated

- a. Login as `root` on Management Server One-Box server or Management Server Primary WebLogic server (Four-Box) - all following commands are executed as `root`
- b. Check the cron job list

```
# crontab -l
```

Example of output when backup is already activated:

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

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

Example of output when backup is not activated:

```
no crontab for root
```

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

2. Activate backup

Run the following commands as `root`:

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

3. Verify if the backup is activated and functional

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

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

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

NSP_BACKUP_TIMESTAMP containing:

- A log file. It contains any information useful to troubleshoot a backup error.

- Database dump and log
 - LDAP backup
 - System files backup.
- c. In the case of four box setup, the NSP_BACKUP dir will contain 4 sub- directories, one for each server of Management Server Four-Box setup. Each of those directories will contain a backup of particular server.

The directory structure is:

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

7.1.1.2 Deactivate Automatic Management Server Backup

This procedure describes how to deactivate automatic Management Server backup.

- a. Login as `root` on Management Server One-Box server or Management Server Primary WebLogic server (Four-Box) - all following commands are executed as root
- b. Check the cron job list

```
# crontab -l
```

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

- c. Edit the contents of the crontab

```
# crontab -e
```

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

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

```
# crontab -l
00 22 * * * . $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd; sh
./LaunchExpNSPd.sh >../trc/cronNSP.log 2>&1
01 00 * * * rm -rf /tekelec/backup`date
\+%\u`;/usr/TKLC/TKLCmf/bin/backup_config backup`date \+%\u` >
/tekelec/TKLCmf/runtime/run/log/backup`date \+%\u`.log
```

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

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

```
/tekelec/TKLCmf/runtime/run/log/backup`date +%u`.log
```

7.1.1.3 Change Automatic Management Server Backup Time and Location

Execute this procedure to change an automatic backup time or location

1. Change Automatic Management Server Backup Time

- a. Login as `root` on Management Server One-Box server or Management Server Primary WebLogic server (Four-Box) - all following commands are executed as `root`
- b. Check the cron job list

```
# crontab -l
```

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

- c. Edit the contents of the crontab

```
# crontab -e
```

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

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

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

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

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

2. Change Automatic Management Server Backup Location

- a. To change the location of where the backup files are stored runs the following command. As `root` run:
- b. Edit the **LaunchExpNSPd.sh** file using a text editor. Replace any occurrence of `/opt/oracle/backup` with a different backup directory.
- c. Save changes.

7.1.2 Management Server Database Backup

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

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

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

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

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

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

This script has three parameters and constraints:

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

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

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

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

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

7.1.3 Realm Backup

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

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

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

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

7.1.4 System Files Backup

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

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

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

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

7.2 Start NSP Service on Primary when Secondary Is Down

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

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

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

7.3 Start NSP Service on Secondary when Primary Is Down

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

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

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

7.4 Configure Apache HTTPS Certificate (Optional)

This procedure describes how to configure the Apache HTTPS certificate.

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

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

```
# su - platcfg
```

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

7.5 Copy Management Backup

1. **Copy Management Server Backup**

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

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

- It will ask for backup user password, enter the password for backup user and press ENTER.
 - **nsp-ip** should be replaced by the Management Server backup server's IP address (Management Server Server or Management Server Oracle server in case of Management Server 4-box configuration).
 - */path/to/backup/dir* should be replaced by exact path of backup on server. For example */opt/backup/backup/NSP_BACKUP_09_13_11_22_00_01*
 - To note exact path of the backup you can use steps mentioned in step 2 below.
 - *local_backup_dir* should be replaced by a directory name of the Customer choosing.
 - After successful completion of the command the backup should be available at the *local_backup_dir* folder.
- In case of any error contact Oracle Support AppendixA. My Oracle Support (MOS)

2. Note down the path of the backup folder on Management Server server.

- a. Login as `root` on Management Server One-Box server or Management Server Oracle server (Four-Box)
- b. Note the path of the backup to be copied by executing the command below:

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

It should output something like:

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

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

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

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

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

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

It should output something like:

```
/opt/backup/backup/ALA_2011_07_01.csv
/opt/backup/backup/ALA_2011_07_12.csv
/opt/backup/backup/ALA_2011_07_23.csv
/opt/backup/backup/ALA_2011_07_02.csv
/opt/backup/backup/ALA_2011_07_13.csv
```

```
/opt/backup/backup/ALA_2011_07_24.csv
/opt/backup/backup/ALA_2011_07_03.csv
/opt/backup/backup/ALA_2011_07_14.csv
/opt/backup/backup/ALA_2011_07_25.csv
```

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

7.6 EPI and Plugin Configuration for Tracing

7.6.1 EPI Configuration

- a) From Internet Explorer, connect to the Management Server Application GUI using the following URL:
http://nsp_ip/nsp
Where nsp_ip is the IP address of the Management Server One-Box server or Management Server Primary WebLogic server (Four-Box).
- b) Login with user Tk1cSrv
- c) Launch ProTrace Application from Applications

7.6.1.1 Configuring Builder Time Tolerance Parameters

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

Builder Time Parameters			
Negative (2-90000):	3 s	Positive (2-90000):	3 s
Guaranteed length (-1-90000):	21600 s		
EPI	Group #	Flex	Enabled
☐ ANumber	1	☒	☒
☐ BNumber	2	☒	☒
Group	3		☒
☐ CNumber		☒	
☐ DNumber		☒	

Add		v	Group#	
------------------------------------	----------------------	----------------------------------	--------	----------------------

- c) Fill in the Builder Time Parameters.
The Builder Time Parameters define the time range used for searching for new xDRs. This time range is related to BEGIN TIME and END TIME of discovered xDRs and uses a Positive and a Negative value.
The ranges for both positive and negative rules are 2-90000 seconds.
The Guaranteed length parameter allows you to enhance the search period to END_TIME + Guaranteed length. This parameter is used for search optimization and corresponds to the longest call or transaction the system is guaranteed to find.
- d) Click on Apply to Save. The Builder Time Tolerance parameters would be saved successfully.

7.6.1.2 Add EPI

- a) Open the EPI Configuration UI and Select a Builder. As in Section 9.8.1.1, a) and b)
- b) Define the EPI's and EPI parameters for that builder.
EPI Name – Select any dictionary field from the drop down.
Group Number – Specify the group number in which you want to add EPI. If group number is blank then the default Group Number during Add operation would be the Max Group Number + 1 (max for the selected builder)
- c) Click Add button. The EPI will get added in the list.
 - Flex and Enabled would be checked by default
- d) Click Apply. The changes are saved.

7.6.1.3 Delete EPI

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

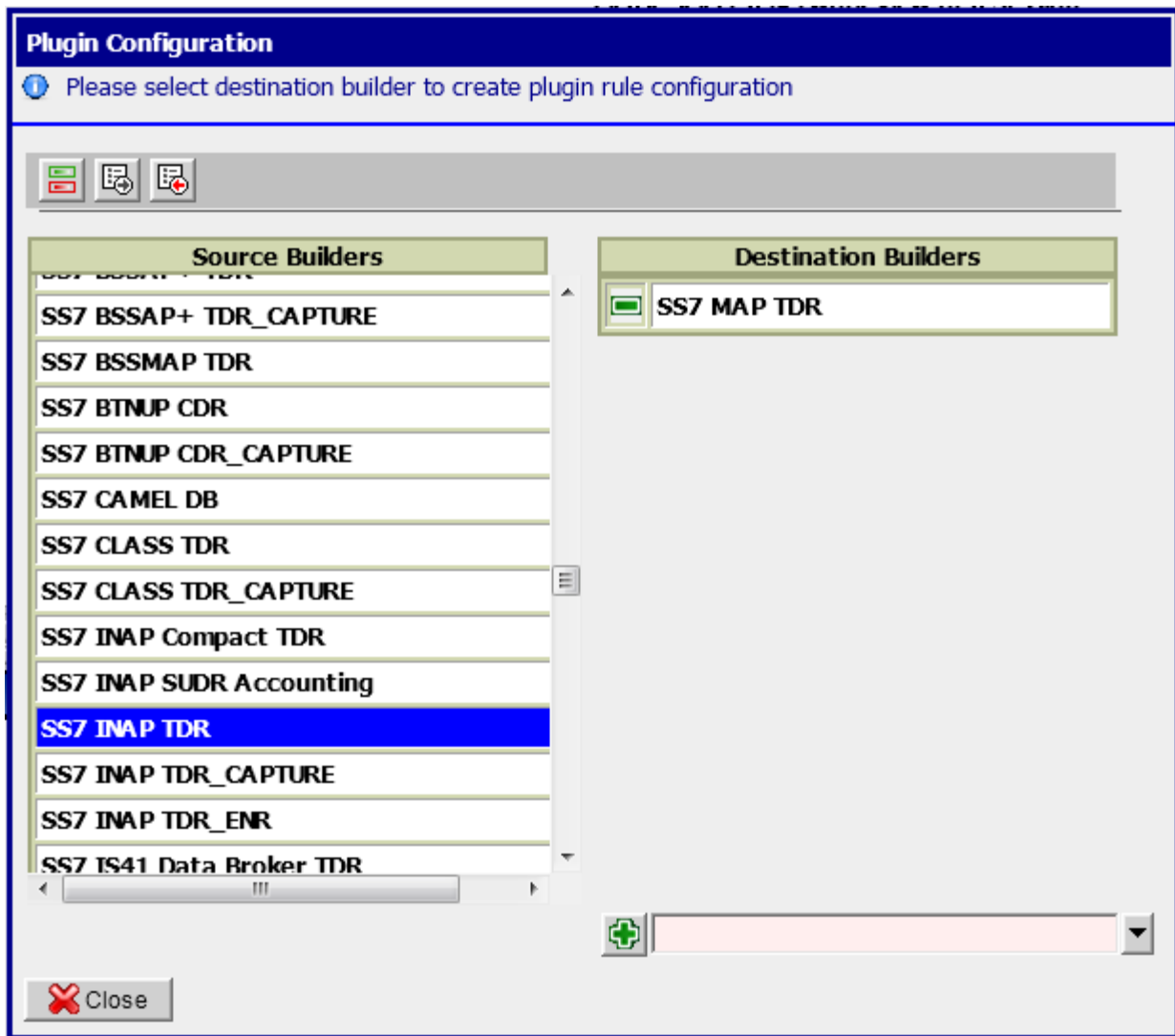
7.6.1.4 Update EPI

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

7.6.2 Configuring Plugins

7.6.2.1 Create Plugin

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



- b) Click on Source Builder to configure. In the right pane all builders mapped with this source builder are populated.
- c) To add a new plugin, select the destination builder from the available builders drop down
- d) Click on Add Button
- e) Plugin Rule Screen will open

Plugin Rule Configuration

Click ok to save auto created plugin rule configuration.

Source:SS7 ISUP ANSI CDR		Destination:SS7 ISUP ETSI CDR	
	A Number		A Number
	B Number		B Number

Please select a field
 Please select a field

Auto-sync reverse couplet ☒

OK
 Cancel

- f) Auto created Plugin Rules for the selected source and destination builders will get displayed. Auto Creation is done for the EPI's which are common to both the builders e.g. if ANumber is an EPI for both Source and Destination Builder a Plugin Rule ANumber → ANumber will be auto created in GUI.
- g) If some auto created rules are not required, user can optionally delete them
- h) If some more rules are required to be added user can optionally add more rules
- i) The Auto-sync reverse couplet Check Box if checked would create a plugin in reverse directionas well when the Plugin is saved
- j) Click on Add Button to create a Plugin Rule after selecting Source and Destination Fields
- k) Click on Ok to Save the Configuration. Plugin would be created.

7.6.2.2 Update Plugin

- a) From Application Menu, Select Configuration > Plugins. The Plugin Configuration screen will be displayed.
- b) Click on Source Builder to configure. In the right pane all builders mapped with this source builder are populated.
- c) Click on the Destination Builder to Edit Plugin
- d) Plugin Rule Screen will be opened
- e) Add/Delete required Plugin Rules
- f) Click on Ok Button.
- g) Plugin would be updated with new rules

7.6.2.3 Delete Plugin

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

7.6.2.4 Export Plugin Configuration

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

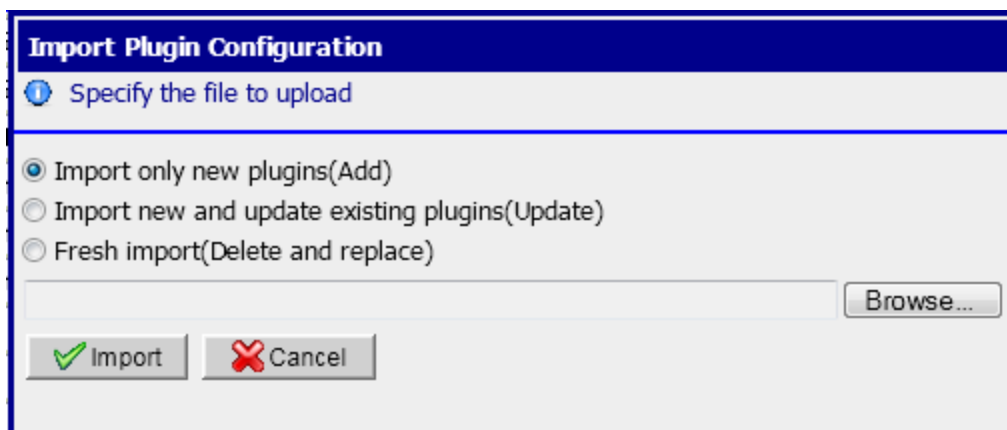
☐ Source	☐ Destination	Builders
☐	☐	SS7 ISUP ETSI CDR_CAPTURE
☐	☐	SS7 ISUP ETSI MULTILEG
☐	☐	SS7 ISUP ETSI SUDR Accounting
☐	☐	SS7 ISUP ETSI SUPER CORRELATION
☐	☐	SS7 ISUP ETSI SUPER CORRELATION_CAPTURE
☐	☐	SS7 IUP CDR
☐	☐	SS7 IUP CDR_CAPTURE
☐	☐	SS7 L2L3 ANSI SUDR
☐	☐	SS7 L2L3 ETSI SUDR
☐	☐	SS7 Ldb TDR

OK Cancel

7.6.2.5 Import Plugin Configuration

7.6.2.5.1 Using GUI

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



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

7.6.2.5.2 Using ant target

- a) Login to nsp-primary box using tekelec user

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

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

where,

<import file path> is the path of the CSV File to Import

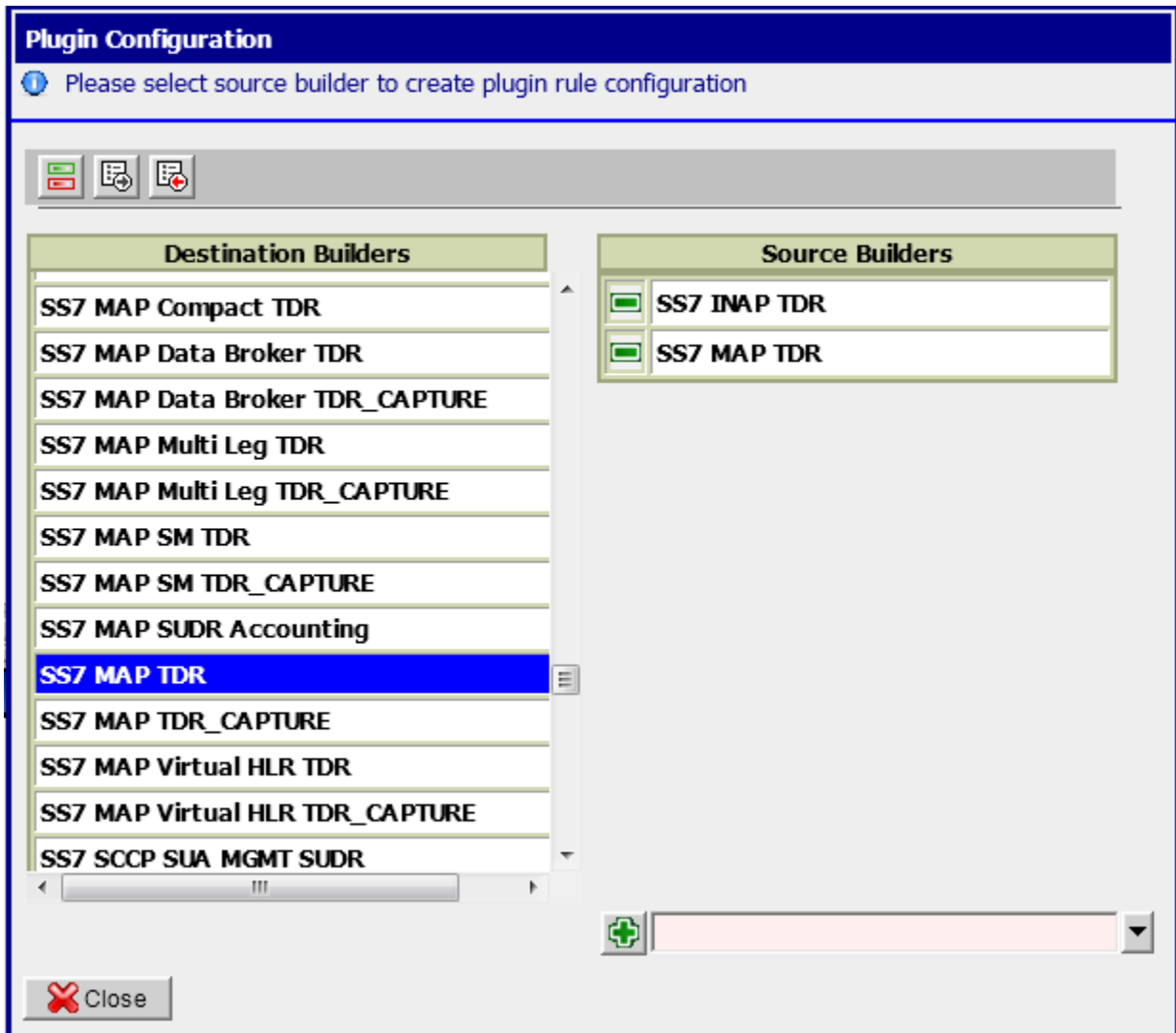
<import type> is the Import Option as described in previous section,

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

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

7.6.2.6 Toggle View Option ‘Switch between Source and Destination View’

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



7.7 Configure HTTPS Certificate on ODA (Optional)

This procedure describes how to configure the HTTPS certificate. The following procedure must be performed on the OTD Admin server. The procedure to configure HTTPS certificate is mentioned in OTD Administration Guide http://docs.oracle.com/cd/E23389_01/doc.11116/e21036/toc.htm. Chapter 11 Manage Security can be referred. Section 11.2, 11.3 and 11.4 should be referred.

7.8 Configure Mail Server (Optional)

This procedure describes how to configure the SMTP mail server on ODA.

Note: On HP similar procedure can be executed from [3]

This procedure is optional; however, this option is required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined)

1. Open a terminal window and log on as root on the Management Admin server and both Managed Servers
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
```

7.9 Configure Authenticated Mail Server (Optional)

This procedure describes how to configure authenticated mail server. This procedure is optional.

Note: On HP similar procedure can be executed from [3]

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 NSP application interface.
2. Log in as weblogic on the WebLogic Console.
3. Select Services ► Mail Sessions ► NspMailSession.
4. Click Lock&Edit and modify the JavaMail properties as needed. For example:

```
mail.transport.protocol=smtp,
mail.smtp.host=mail.server,
mail.smtp.from= noreply@tekelec.com,
mail.smtp.timeout=1000,
mail.smtp.connectiontimeout=1000
```

5. Add the following parameters:

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

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

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

```
mail.smtp.socketFactory.port=4 6 5
mail.smtp.socketFactory.class=javax.net.ssl.SSLSocketFactory
mail.smtp.socketFactory.fallback=false
```

7. Click Save.
8. Click Activate Configuration.
9. Perform section 6.3.1 from [\[4\] PIC 10.1.5 Installation document](#),

7.10 Configure SNMP Management Server (Optional)

This procedure describes how to configure the SNMP on management server ODA.

Note: On HP similar procedure can be executed from [3]

This procedure is optional; however, this option is required for Forwarding (forwarding by SNMP filter defined)

1. Log in as root user on the ODA Oracle server and run below mentioned script.

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

This script will prompt for Oracle server external IP, Weblogic Admin server internal IP, SNMP server IP and version. Provide them very carefully. The script shall update the configuration in /etc/snmp/snmpd.conf file

2. Log in as root user on the weblogic Admin Server and perform following steps.

```
a) Open AgentMbean.properties file
# vi /opt/TKLCjmxagent/in/AgentMBean.properties
b) Add Following lines in the file and save the file
SnmpAgentHost=<IP Address of Oracle Server>
SnmpAgentPort=705
c) Restart jmx agent service
# service jmxsd restart
```

7.11 Modify WebLogic Administration Password (Optional)

Note: On HP similar procedure can be executed from [3]

Once user has changed the password of weblogic on ODA, following steps has to be executed on NSP Admin server so that NSP applications can adapt that change.

- 1) Log on to NSP Admin Server as root user and execute below scripts

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

This script will prompt for database user(NSP) password and weblogic console new password. Provide them very carefully.

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

This script will prompt for Admin server IP, Admin server port, weblogic console username and weblogic console new password. Provide them very carefully.

- 2) Restart NSP service

```
# service nspservice restart
```

7.12 Modify Oracle VM IP (Optional)

On ODA, except for Oracle server the internal IP address for weblogic VMs are maintained in the database. So the below procedure should be executed if the external IP address of the oracle server is changed.

Note: No need to execute this script if weblogic VMs external IPs are changed.

Note: This procedure is only applicable on ODA.

Once user has changed the external IP of oracle box, following steps has to be executed on NSP Admin server so that NSP applications can adapt that change.

- 1) Log on to NSP Admin Server as root user and execute below steps

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

```
# sh updateIPAddressOracle.sh <dbusername>/<dbuserpassword> <oldIP> <newIP>
```

- 2) Restart NSP service

```
# service nspservice restart
```

7.13 Configure Session Timeout (Optional)

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

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

7.14 Control HTTPS Access of Management server on ODA (Optional)

This procedure describes how to control the access (enable or disable) of the management server frontend to HTTPS. This procedure is optional. The procedure(s) mentioned in OTD administration guide should be executed for enabling/disabling HTTPS access. http://docs.oracle.com/cd/E23389_01/doc.11116/e21036/toc.htm. Section 11.2, 11.3 and 11.4 should be referred.

Enable HTTPS access (No Listener for port 443 is present)

Note: All the steps must be performed using the OTD Admin Console.

1. Login to OTD Admin Console.
2. Create a new http listener with port 443. Follow the chapter **10.1 Creating a listener** in [7].
3. Configure the SSL for a listener Enable the SSL. Follow the chapter **11.2.2 Configuring SSL/TLS for a Listener** in [7].
The self signed certificates can be used in step3. Refer **11.4.1 Creating a Self-Signed Certificate**
4. Save and Deploy the configuration.
5. Check the OTD access with https e.g. [Error! Hyperlink reference not valid.](#)

Note: By default the http access is already present. The https access will not disable the http access.

Enable HTTPS access (Listener with port 443 is already present)

Note: All the steps must be performed using the OTD Admin Console.

1. Login to OTD Admin Console.
2. Select and modify the http listener with port 443.
 - a. Enable the listener by following the chapter **10.3 Modifying a listener** in [7].
 - b. Enable SSL access if not already enabled.
3. Save and Deploy the configuration.
4. Check the access with https is enabled now. e.g. [Error! Hyperlink reference not valid.](#)

Note: By default the http access is already present. The https access will not disable the http access.

Disable HTTPS access

Note: All the steps must be performed using the OTD Admin Console.

1. Login to OTD Admin Console.

2. Select and modify the http listener with port 443.
 - a. Disable the listener by following the chapter **10.3 Modifying a listener** in [7] .
3. Save and Deploy the configuration.
4. Check the access with https is disabled now. e.g. **Error! Hyperlink reference not valid.**

Disable HTTP access

Note: All the steps must be performed using the OTD Admin Console.

1. Login to OTD Admin Console.
2. Select and modify the http listener with port 80.
 - a. Disable the listener by following the chapter **10.3 Modifying a listener** in [7] .
3. Save and Deploy the configuration.
4. Check the access with http is disabled now. e.g. **Error! Hyperlink reference not valid.**

Enable HTTP access

Note: All the steps must be performed using the OTD Admin Console.

1. Login to OTD Admin Console.
2. Select and modify the http listener with port 80.
 - a. Enable the listener by following the chapter **10.3 Modifying a listener** in [7] .
3. Save and Deploy the configuration.
4. Check the access with http is enabled now. e.g. **Error! Hyperlink reference not valid.**

7.15 Configure External LDAP (Optional)

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

1. Open a terminal window and log in as root on the Management server (One-box).
2. Configure the NSP database. As root, run:


```
# cd /opt/nsp/scripts/procs
# sh nsp_update_procs.sh externalLDAP true
```
3. From a web browser, connect to the NSP application interface. Use the following URL:


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

 where 192.168.1.1 is the IP address of the Management server.
4. Log in to the WebLogic Console as weblogic.
5. Select Security Realm ► myrealm ► Providers ► Authentication.
6. Click Lock&Edit and add a new LDAP Authenticator.

Provide the necessary parameters that correspond to the customer LDAP tree configuration (refer to the WebLogic 10.3.6 documentation(**E23943_01**) for more information about this process).
7. Set the control flag for all of the Authentication Providers to SUFFICIENT.
8. Click Save.
9. Click Activate Configuration.

7.16 Control Cisco PMP (Optional)

This procedure describes how to enable or disable the Cisco PMP on ODA. This procedure is optional.

Note: On HP similar procedure can be executed from [3]

1. Open a terminal window and log in as root on the Management Admin Server.
2. su - tekelec
3. Run the appropriate commands:

- To enable the Cisco PMP, run:

```
# cd /opt/nsp/nsp-package/framework/db/dist/utlis/cmd
# sh PmpOption.sh -e
```

- To disable the Cisco PMP, run:

```
# cd /opt/nsp/nsp-package/framework/db/dist/utlis/cmd
# sh PmpOption.sh -d
```

Note: Session logout is required to make the change effective.

7.17 Configure the default settings for the new users (Optional)

This procedure describes how configure the default settings for the new users. This procedure is optional.

1. Login on the NSP GUI as user tekelec
2. Modify the user preferences according the customer requirement and especially the Time Zone.
3. Validate the settings using the button “Save as default” for each panel you modified.

7.18 Configure CSV streaming feed feature (Optional)

This procedure describes how to enable or disable the CSV streaming feed feature: this feature is subject to subscription and it is disabled after installation.

Note: On HP similar procedure can be executed from [3]

1. Open a terminal window and log in as tekelec on the Management server Admin Server
2. Run the appropriate commands:

- To enable CSV streaming feed, run:

```
# cd /opt/nsp/nsp-package/framework/core
# ant enable.csv.license
```

- To disable CSV streaming feed, run:

```
# cd /opt/nsp/nsp-package/framework/core
# ant disable.csv.license
```

7.19 Configure FSE automated update (Optional)

This procedure describes how to enable or disable the automatic update of enrichment configuration file defined or to be defined in Management system.

NSP scan regularly defined folder and its subfolder (every 30 mn) to find files with same name as the those declared. In this case it loads file to replace exsiting FSE and reapply it automatically to selected session.

1. Log in as tekelec on the NSP application interface.
2. Select the Centralized Configuration application.
3. Select Mediation ► Enrichment Files.

The Enrichment Files List screen opens

4. Click on automated update button in list toolbar .

The FSE Auto Update Configuration screen opens.

5. Enter SFTP location where system can find Enrichment FSE file.

URL should be like `sftp://<USER>:<PASSWORD>@<HOSTNAME_OR_IP>/<PATH>` where

- <USER> is username of SFTP server
- <PASSWORD> is password of SFTP user
- <HOSTNAME_OR_IP> is address of SFTP server
- <PATH> is relative path under user home folder in SFTP server

Note: Empty string turns off automated update

6. Click OK to validate changes.

7.20 Configure NSP FTP or SFTP Server

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

Note: For an Management Server Four-box, this procedure needs to be run on both the Primary server and the Secondary server.

1. Copy the FTP security file from the Management Server server

- a) Open a terminal window and log in as root on the Management server (One-box), Primary/Secondary server (Four-box), Managed Server1 and Managed Server2 on ODA.
- b) As root, run:

```
# cd /opt/nsp/bea/user_projects/domains/tekelec/nsp
```
- c) Copy the contents of file `sftp_security.pub`.

2. Update the FTP or SFTP server

- a) Log in on the FTP or SFTP server.
- b) In the file `$HOME/.ssh/authorized_keys`, add the contents of file `sftp_security.pub` that you copied in the previous step.
- c) Make sure that the FTP or SFTP server is properly configured to allow file transfer.

Don't use root user to transfer files. tekelec and other users should be use.
By default files will be uploaded to user home. E.g- /opt/nsp for tekelec

7.21 Management Server One box Installation on HP

For the installation procedures of management server refer section 2.3 in [\[3\] PIC 10.1.0 Installation Document](#),

Note: Refer chapter 6.3.7 Change Customer Icon from [\[4\]](#) for updating the customer icon on HP based installation.

7.22 Weblogic Console access on https on ODA(Optional)

The procedure should be executed on the on the OTD admin console to configure the OTD to access the weblogic console using OTD.

1. Login to OTD Admin Console

2. Create a new origin server pool, Follow chapter **6.1 Creating Origin Server Pool** in [7] . Use the internal IP address (e.g.192.168.16.64) of the Weblogic Admin Server and port 7001 as details for origin server.
3. Save the configuration and deploy it.
4. Create a new route under the existing Virtual Server, Refer Chapter **8.4 Configuring Routes** in [7] .
 - a. Select the origin pool created for admin server in step2.
 - b. Add the condition in route URI, **\$uri ~ "^/console"** i.e. prefix with /console to the new origin server pool
5. Save the configuration and deploy.
6. Test the https access to Weblogic console using **Error! Hyperlink reference not valid.**

8 Acquisition Maintenance Procedures

8.1 Procedure to enable/disable timestamp resolution to nanoseconds

This procedure describes how to enable/disable the timestamp resolution to ns on transport for IPRaw packet between Probed and Mediation.

By default, this feature is enabled and the default timestamp resolution is the nanosecond.

This feature can be activated separately for MFP or DTS transport protocol by the parameter 'TlvDsMask' inside the 'LongParam' table:

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

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

Note: A clobber on the Acquisition server will reset the default value for this feature which is "2-TLV_DTS_IP" in this feature.

8.2 Falco Firmware upgrade procedure

Use the Document [WI006872](#) at the end of the procedure, displayed version must be:

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

8.3 Key exchange procedure with Neptune probe

This procedure must be applied after a fresh install or upgrade of the Neptune probe.

It must applied on Management Server servers for Management Server 1 box and on both Primary WebLogic and Secondary WebLogic servers in case of Management Server 4 boxes

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

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

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

x.x.x.x is the administration IP address of the Neptune probe

2. Import of the key
 - a. Run the command :

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

x.x.x.x is the administration IP address of the Neptune probe

For Password : enter 'DemoTrustKeyStorePassPhrase'

Answer Yes when it is asking if the certificate is reliable

3. Restart the server
 - a. In case of Management Server 4 boxes, the following command must be run only when the steps below were applied on all WL servers
 - b. Run the command (for Management Server 4 boxes, run this command only on the Primary WebLogic server):

```
$ service nspservice restart
```

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

For deleting the import

1. Run the command :

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

x.x.x.x is the administration IP address of the Neptune probe

2. Remove the file Neptune.crt under /tmp
3. Rerun import (step 2 and 3 above)

8.4 Add New Server in the Integrated Acquisition sub-system

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

1. Install Integrated Acquisition server
 - a. **Install** the additional Integrated Acquisition server using the procedures mentioned in Chapter 5 in PIC 10.1.5 Installation document, . Only procedures till section 7.3 should be executed.
Note: Use the bulkconfig file already present on the already installed servers and add the entry for the additional Integrated Acquisition server in the bulkconfig file. Copied the modified bulkconfig file to all the other Integrated Acquisition servers.
Run bulkconfig script as root user on all subsystem servers:

```
# /opt/TKLCmf/bin/bulkConf.pl
```
2. Discover the server on Management Server
 - a. **Log in to the Management Server application**
 - i. Log in as tekelec to the Management Server application interface using the Management Server IP address.
 - ii. Click **Centralized configuration**. The Management Server application launches.
3. Discover the server on Management Server
 - a. **Modify Integrated Acquisition site on Management Server**
 - i. Select **Equipment Registry ► Sites**
 - ii. Navigate to **XMF**
 - iii. Right click in the requested subsystem
 - iv. Select **Add** from the popup menu.
 - v. Fill in the **Host IP Address** field with the IP address of the server you want to add.
 - vi. Click the **Create** button.
 - vii. Return to the **Equipment registry**.
Click on the subsystem to display the list of servers.
 - viii. Choose the newly added server and press **Discover applications**.
4. Apply Configuration on Integrated Acquisition
 - a. **Apply Changes on Integrated Acquisition site on Management Server**
 - i. Navigate to the Mediation view.

- ii. Navigate to Sites
- iii. Open XMF and right-click on the subsystem.
- iv. Select Apply changes... from the popup menu.
- v. Click on the Next button
- vi. Click on the Apply Changes button.
- vii. Wait until changes are applied.
- viii. Verify that result page does not contain any errors.

8.5 Change the hostname of the Probed Acquisition Server

The procedure should be executed for the Probed Acquisition server in case there is a need to change the hostname of the server. Following steps must be executed for changing the hostname of the server:

1. Update "/root/bulkconfig" file with new hostname
2. Run bulkconfig script as root user:

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

Warning: On changing the hostname of the server, the bulkConf.pl script automatically clobber the IDB of the probed acquisition server. This is done to clean the configuration of the previous hostname. The subsequent Apply Change will restore the configuration on the server.

3. Reboot the server
4. Sync the new hostname on the Management Server ProAdmin.
 - a. Login to Management Server GUI as privileged user and open Centralized Configuration application.
 - b. To synchronize, go to Equipment Registry->sites->XMF and select select XMF subsystem to update. A table with the list of all servers is displayed (see picture below)
 - c. Select the xMF server and click on Discover Applications.

The screenshot shows the 'Network software platform' GUI. The breadcrumb navigation is 'Equipment Registry > Sites > IMF10_BM > XMF > IMF10_BM:XMF > List'. A table displays the following data:

#	Host Name	Description	Discover Applications	Position	IP Address
1	IMF1002-1A		1	1	10.250.47.133
2	IMF1002-1B		1	2	10.250.47.134
3	IMF1002-1C		1	3	10.250.47.135

5. Apply Change
 - 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.

8.6 Remove Server from the Integrated Acquisition sub-system

The procedure should be executed for the Integrated Acquisition sub-system in case there is a need to remove server from the Integrated Acquisition sub-system. Following steps must be executed for removing the server from the already installed Integrated Acquisition sub-system:

1. Remove the server from Acquisition Perspective on Management Server
 - a. **Log in to the Management Server application**
 - i. Log in as tekelec to the Management Server application interface using the Management Server IP address.
 - ii. Click **Centralized configuration**. The Management Server application launches.
 - iii. Go to Acquisition->Site->xMF (sub-system)->Servers
 - iv. Select the server and click on delete icon
2. Remove the server from Equipment Registry on Management Server
 - a. **Modify Integrated Acquisition site on Management Server**
 - i. Select **Equipment Registry ► Sites**
 - ii. Navigate to **XMF**
 - iii. Click in the requested subsystem
 - iv. Select the Server on the right screen
 - v. Click the **Delete** icon.
 - vi. Return to the **Equipment registry**.
3. Modify the bulkconfig file on all the existing servers in the sub-system.
 - a. **As root, update “/root/bulkconfig” file to remove the server entry.**
4. Execute the bulkconf.pl script on each existing server in the sub-system
 - a. As root user, run

```
# /opt/TKLCmf/bin/bulkConf.pl
```
5. Apply Configuration on Integrated Acquisition Subsystem
 - a. **Apply Changes on Integrated Acquisition site on Management Server**
 - i. Navigate to the Mediation view.
 - ii. Navigate to Sites
 - iii. Open XMF and right-click on the subsystem.
 - iv. Select Apply changes... from the popup menu.
 - v. Click on the Next button
 - vi. Click on the Apply Changes button.
 - vii. Wait until changes are applied.
 - viii. Verify that result page does not contain any errors.

9 Mediation Maintenance Procedures

Note: It may be require to give root ssh access before executing many procedures. Please give the access and then revoke it after completing the procedures, as mentioned below

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit
```

```
# /usr/TKLC/plat/sbin/rootSshLogin --revoke
```

9.1 Offload DFPs from the Mediation Server

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

1. Redistribute processes

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

2. Redistribute DataFeed

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

3. Cancel KPI historical tasks

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

4. Reassign external connections

Note: The steps before take care about the stream tracking and if a producer dataflow processing has moved to another server, the consumer dataflow processing will finish

processing the buffered data on the first server and automatically reconnect on the newly assigned server. But this automatic procedure does not apply to external connections.

- a) Acquisition probe (Integrated Acquisition, Probed, MSW) sending data to a stream on this machine.

In such a case it is required to reconfigure also this system in order to reconnect to the replacement (in general the spare) server

- b) Other Mediation subsystem processing output data from this subsystem.

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

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

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

9.2 Configure PDU Storage Parameters

- a) Log into any server from Mediation subsystem

- b) As `cfguser` run:

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

Example output:

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

The output will show you information about ActMaster and StbMaster of the subsystem

- c) On ActMaster server, type:

```
$ ivi SubsystemTaskParam
```

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

```
#!/bin/sh
iload -ha -xU -fID -fParamName -fParamValue SubsystemTaskParam \
<<'!!!!'
1|AlarmClear|1500
2|AlarmFail|1500
3|MaxFileAge|864000
4|MaxPercentUsage|90
5|ExcludePath|write.enable
6|Path|/opt/TKLCixp/pdu
7|Interval|5
8|Interval|300
9|Path|/es
10|ExcludePath|statistics
11|LoginName|ixp
13|AlarmFail|100
14|AlarmClear|100
15|OracleMaxPurgeTime|900
16|IdbPurgeTime|21600
17|TaskPurgeTime|604800
18|ExcludePath|run
19|DatabaseName|ixp0008-1a_DWH
20|HostName|ixp0008-1a
21|Password|IXP
```

```
!!!!
```

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

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

```
$ pm.kill IxpPurge
```

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

9.3 Enable/disable Write Access to the PDU Mounts

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

1. To disable writing

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

```
# su - platcfg
```

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

2. To enable writing

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

```
# su - platcfg
```

- b) Navigate to **IXP Configuration** ☉ **PDU Storage** and press **Edit**
- c) Mark both PDU mounts to **yes** to enable writing.
Note: After this step the IxpBuild processes will be able to write to its PDU mounts from a specific PDU Storage Server.

For ZFS storage following should be done to enable/disable Write acces for PDU mounts.

- a) To enable write access, touch `write.enable` in the shared directory on the mediation server
- b) To disable weite access, `rm write.enable` in the shared directory on the mediation server.

9.4 Set Behavior Mode for DWS Server

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

Note: In case of single DWS server in a storage pool, the following steps must not be performed.

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

9.5 Re-Sync the Mediation Configuration

This procedure describes how to synchronize the Mediation configuration from the Management Server. This procedure is applicable to the Mediation ActMaster server.

1. Drop synchronization history on the Mediation ActMaster server

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

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

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

2. Run Apply Changes to Mediation subsystem from Management Server

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

9.6 Add Server to the Mediation Subsystem

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

This procedure is applicable to the Mediation:

- Mediation Base Server
- Mediation PDU Storage Server

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

1. Integration with the Mediation subsystem

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

- a) Open a terminal window and log in on Mediation server you are about to add to the Mediation subsystem as `root`.
- b) Update the `/root/bulkconfig` file.
Note: The easiest way how to update the bulkconfig file is to copy the bulkconfig file from any server of the target Mediation subsystem. Store this file to new Mediation server. Then add the `host` line with newly installed Mediation server to the bulkconfig file. Check that the bulkconfig file on the additional Mediation server now contains overall subsystem

configuration information and also make sure that the bulkconfig files contains records for all servers in the subsystem including the newly added one.

- c) Once your bulkconfig is valid run automated integration script:

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

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

In this case run the following as root:

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

And repeat the step again.

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

Run the following steps:

1. As root run:

```
# bc_customer_integration.sh --local
```

2. Once finished server will reboot.

3. Log in back to the same newly added server. As root run:

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit  
# bc_adjust_subsystem.sh
```

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

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

2. Install the xDR Builder package

An xDR builder package must be associated to the particular subsystem before running this procedure. All servers in the subsystem must have the same xDR builders' package.

As `cfguser` run:

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

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

3. Add server to existing Mediation subsystem

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

4. Apply configuration to the Mediation subsystem

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

5. Verify license installation

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


```
$ IxpCheckLicense
```
- c) Verify the output.
The information about the license should state that license is valid and that license type is not STARTUP. If the license type is STARTUP contact the AppendixA. My Oracle Support (MOS)

9.7 Add Mediation Server to the Mediation Subsystem in Management/CCM

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

1. Add server to existing Mediation subsystem

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

2. Apply configuration to the Mediation subsystem

- a) Navigate to the **Mediation** view.
- b) Navigate to **Sites**
- c) Open **IXP** and right-click on the subsystem.
- d) Select **Apply changes...** from the popup menu.
- e) Click on the **Next** button
- f) Click on the **Apply Changes** button.
- g) Wait until changes are applied.

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

9.8 Remove Server from the Mediation Subsystem

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

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

1. Offload the Mediation server

Offload DFPs from the server you are about to remove from the subsystem. Refer to [9.1 Offload DFPs from the Mediation Server](#)

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

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

Shutdown this server. As `root` run:

```
# poweroff
```

3. Remove the xDR builders from the Mediation subsystem in Management

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

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

4. Remove server from the Mediation subsystem in Management Server

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

This will remove the Mediation server from the Mediation subsystem.

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

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

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

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit
# bc_adjust_subsystem.sh
```

- d) Run analysis to see if the subsystem has been adjusted

properly. As root run:

```
# bc_diag_bulkconfig -a
```

Note: Clobber the server using “prod.start -c” which was removed. It will be necessary to clobber the server before it can be reused in any other sub-system.

9.9 Change Mediation network interface type to Bonding

This section describes the Mediation type network interface change procedure for PIC system. This type interface change procedure is applicable to already configured PIC system that is in running state.

This section describes the IXP type network interface change procedure for PIC system. This type interface change procedure is applicable to already configured PIC system that is in running state.

Note: In case of bonding, if any of the interface is down e.g. eth01 or eth02, then no alarm will be raised by the platform or the application.

1. Delete old interface eth0X

- a. To delete the default route, as root, run:

```
netAdm delete --route=default --device=eth01 --gateway=<gateway-ip>
```

- b. To delete the Vlan interface, as root, run:

```
netAdm set --device=eth01 --address=<ip-address> --deleteAddr
```

2. Configure the bonding interface

- a. To check if bonding interface exist, as root, run:

```
netAdm query --device=bond0
```

- b. If bonding interface exist, as root, run:

```
netAdm set --device=bond0 --bootproto=none --type=Bonding --addr=<ip-address> --  
netmask=<network-mask> --onboot=yes --mode=active-backup --miimon=100 --  
bondInterfaces=eth01,eth02
```

If bonding interface not exist, as root, run:

```
netAdm add --device=bond0 --bootproto=none --type=Bonding --addr=<ip-address> --  
netmask=<network-mask> --onboot=yes --mode=active-backup --miimon=100 --  
bondInterfaces=eth01,eth02
```

- c. To create the default route, as root, run:

```
netAdm add --route=default --device=bond0 --gateway=<gateway-ip>
```

- d. Restart the network, as root, run:

```
service network restart
```

3. In the **bulkconfig** file, be sure to use the bond0 interface (and not the usual ethxx interface)

- a. Login to the iLO as root of any IXP server in the subsystem you are about to reconfigure
b. Update the /root/bulkconfig file with the new interface

4. Run **Apply change** procedure

- a. Run the IXP subsystem customer integration procedure as root:

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit  
# bc_customer_integration.sh
```

9.10 Installation of External Datawarehouse

This procedure describes how to adapt the customer Oracle server to the External DatawareHouse for either the DataExport feature (Oracle To Oracle feeds) or the Oracle streaming feeds.

The customer Oracle server that is dedicated to be an External Datawarehouse need to fulfill the following prerequisites:

- Oracle 10g or 11g must be installed

Note: Take care of using the same Oracle Database release as the one running on the DWS (or internal DWH). If the DWS run Oracle Database 11g, use Oracle Database 11g for the external DWH; if the DWS run Oracle Database 10g, use Oracle Database 10g for the external DWH.

- Database instance must be created with login and password
- 4 tablespaces must be created:
 - data tablespace with name DATA_CDR
 - index tablespace with name DATA_IND
 - configuration tablespace with name DATA_CONF
 - log tablespace with name DATA_LOG

1. Customer: Grant roles

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

Run the following commands in Oracle console:

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

2. Create the schema

From any Mediation server, as *cfguser*, run:

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

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

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

3. Post-installation check

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

Verify you can access External DataWarehouse console. From any Mediation server, as

cfguser, run:

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

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

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

```
SQL> desc dataserversession;
```

You should receive the output similar to the following:

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

Quit Oracle console:

```
SQL> quit
```

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

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

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

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

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

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

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

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

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

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

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

5. Tune the External Datawarehouse / Oracle feeds feature

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

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

```
$ cd /opt/TKLCixp/prod/db/tuning/cmd
$ ./CreateJobClass.sh sys/sys_password@ip/sid
$ ./SystemStats.sh sys/sys_password@ip/sid -i
$ ./TuningPackage.sh user/password@ip/sid -i
$ ./FlushSharedPool.sh sys/sys_password@ip/sid
$ ./ModifyMaintenanceWindow.sh sys/sys_password@ip/sid 2 4
```

On Oracle 10g only:

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

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

6. Revoke DBA role

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

9.11 Setup NFS Mount for DataFeed Application on Customer Provided Server

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

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

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

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

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

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

2. Create export directories

Note: Run this step on customer provided server.

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

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

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

3. Update the `/etc/exports` file

Note: Run this step on customer provided server.

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

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

4. Restart the NFS service

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

As root run:

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

5. Update the `/etc/hosts`

Note: Run this step on customer provided server.

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

6. Configure the DataFeed Application (Management Server)

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

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

9.12 External Storage Configuration using NFS on ODA

The external storage can be configured on the ODA for the PDU storage using NFSv4. Procedure to configure NFS mount point on ODA Oracle Server:

1. Create PDU storage directories as root user

```
# cd /cloudfs
# mkdir -p  export/pdu_1
# chmod 766 /cloudfs/export/pdu_1
```

2. Update the `/etc/exports` file as root user

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

```
/cloudfs/export/pdu_1 ixp????-??(rw,async,no_root_squash,anonuid=-1)
```

3. Update the `/etc/hosts`

Note: Run this step on ODA oracle server.

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

As root, edit the /etc/hosts file using vi editor and add the following line for all the mediation servers. Save the file after modification.

```
<ip_address>      <mediation_server_hostname>
For example
10.31.2.61         ixp9010-1a
10.31.2.62         ixp9010-1b
```

4. Restart the NFS service

As root run:

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

9.13 Mediation Server Installation on Blades

Refer and follow the flow defined in Section 2.8 “IXP DL360/BL460c Gen8” in [PIC10.1.0 Installation Guide](#) for the mediation server installation on Blades and RMS HP hardware.

9.14 DR Storage installation on HP

The procedure given below is applicable to both RMS and blades.

Refer and follow the flow defined in Section 2.7 “DWS DL360/BL460 Gen8” in [PIC10.1.0 Installation Guide](#) for the DWS installation on Blades and RMS HP hardware.

9.15 Data Record Storage Post-Integration Configuration (Optional)

The procedure is applicable for both ODA as well as HP based DWS.

9.15.1 Activate Session Compression

This procedure describes how to activate/deactivate compression for a particular Oracle session.

Before performing this procedure be aware of the following facts:

- Activated compression will have negative influence on storage speed rate.
- Activated compression will have negative influence on ProTrace queries speed rate.
- Activated compression will have positive influence on storage size.
- All current benchmark tests have been tested with deactivated compression.

Note: Execute this procedure for all DWS servers in the Storage Pool where the session is located, from any remote mediation base server.

1. Login to the any mediation server

- a) Open a terminal window and log in to the mediation server as cfguser.
- b) Navigate to /opt/TKLCixp/prod/db/tuning/cmd directory. As cfguser run:

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

2. How to activate the compression

To activate compression for particular session as cfguser run:

```
$ ./TuningPackage.sh ixp/ixp@<IP>/ixp -c <session>
```

where <IP> is the IP of DWS server and <session> is the name of particular session.

3. How to deactivate the compression

To deactivate compression for particular session as cfguser run:

```
$ ./TuningPackage.sh ixp/ixp@<IP>/ixp -x session
```

where <IP> is the IP of DWS server and <session> is the name of particular session.

4. Verify the settings

Verify the session list where the session compression is activated. As cfguser run:

```
$ ./TuningPackage.sh ixp/ixp@<IP>/ixp -l
```

Where <IP> is the IP of DWS server.

All session with activated compression will be listed in the command output.

9.15.2 Change Default Passwords of Oracle Accounts (optional)

This procedure describes how to modify the default passwords of the Oracle account. This procedure is applicable to any DWS server in the subsystem.

1. Connect as database administrator

a) Log in on the DWS server.

b) Connect to Oracle as the database administrator.:

```
# su - oracle
# export ORACLE_SID=IXP
# ORAENV_ASK=NO source oraenv
# sqlplus / as sysdba
```

2. Set passwords

a) Set the password for DBSNMP. Run:

```
SQL> alter user DBSNMP identified by password;
```

where password is actual password.

b) Set the password for OUTLN. Run:

```
SQL> alter user OUTLN identified by password;
```

where *password* is actual password.

c) Set the password for SYSMAN. Run:

```
SQL> alter user SYSMAN identified by password;
```

where password is the actual password.

3. Close the Oracle session

Exit the Oracle session. Run:

```
SQL> exit;
```

10 Platform based Maintenance Procedures

10.1 PM&C Disaster Recovery

Refer to PM&C Disaster Recovery procedure in [PM&C Disaster Recovery](#)

10.2 Install Operating System on G6 Rackmount Servers

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

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

Note: This procedure needs to be executed only for Acquisition G6 servers.

Note: This procedure describes a re-installation of Operating System in case of Disaster Recovery procedure. The BIOS configuration procedures which have been already executed during the fresh installation are not described.

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

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

2. **Install the operating system**

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

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

3. **Reboot the server**

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

If the installation did not complete successfully, contact the Oracle Support, AppendixA **My Oracle Support (MOS)**

10.3 Install Operating System on Gen8 Rackmount Servers

Refer to installation of operating system procedure described in [2]

10.4 Install Operating System on E5-APP-B Servers

Refer to installation of operating system procedure described in [2]



It is recommended to use the “scrub” option to IPM the E5-APP-B card in order to avoid any issue introduced by software RAID mechanism.
Recommended command: “TPDIvm scrub”

10.5 IPM Blade Servers Using PM&C Application

1. **IPM Servers Using PM&C Application**

Refer to IPM procedure using PM&C application in [Platform Configuration Procedure Reference](#)

2. **Additional configuration step after IPM**

This step is mandatory on all blades server after IPM.

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

1. Connect as root user on the blade

2. Run

```
# rcstool co /etc/sysctl.conf
```

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

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

4. Run

```
# rcstool ci /etc/sysctl.conf
```

10.6 Switch Disaster Recovery

Refer to **APPENDIX: Switches Configuration** in E53508-01 PIC 10 installation Procedure

Note: Take care to check in any customer specific config was applied

11 External Software Configuration

11.1 Java Runtime settings

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

1. Update to the latest JRE (version 7 update 51 or later)
2. Configure Runtime parameters
 - Go to Start Menu ► Control Panel ► Java
 - Select the Java tab and click on View button
 - Here, you will find Java Runtime parameters remove any memory parameter (-Xmx or -Xms)
3. As security rules have been enforced in order to run applets (ProAlarm config), configure Exception Site List in Security parameters
 - Go to Start Menu ► Control Panel ► Java
 - Select the Security tab
 - Click on Edit Site List ► Add
 - Enter Management Server URL like **Error! Hyperlink reference not valid.**>

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

11.2 IE Browser Settings

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

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

1. Force Refresh

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

- f. Click on **OK** on Internet Options window.

2. Scripting

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

3. Auto resize popup windows

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

4. Allow windows without address bar

Setting needs to be done for IE7 only.

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

5. Enable Downloads

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

6. Configure IE to have more than two download sessions

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

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

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


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

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

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

- f. Quit Registry Editor

7. Enable Active Scripting

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

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

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

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

9. Enable Applet Table Format For ProTrace

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

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

10. ActiveX Controls

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

11. Clear History

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

12. Compatibility view

Note: This step needs to be done for IE9

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

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

12 Knowledge Base Procedures

12.1 How to mount the ISO file via iLO

Note: For latest procedure to mount ISO corresponding to iLO4, please refer platform configuration guide [1]

1. Store the ISO file to the local disk.
2. Open a web browser and enter the IP address of server iLO. After security exception a login page will appear. Log in as `root`.
3. Navigate to the **Remote Console** tab.
4. Click on Integrated Remote Console.
An Integrated Remote Console window appears.
5. Click on **Virtual Media** which is visible in blue bar at the top of the **Integrated Remote Console** window.
6. Navigate to **Image** with a small CD-ROM picture on the left side. Click on **Mount**.
A window will pop up asking for the ISO path. Navigate to the ISO file and click **Open**.
7. Now the ISO file is mounted on a target server as a virtual CD-ROM. Such new device will appear under `/dev/` directory.

To find the new virtual CD-ROM media run on a target server as `root`:

```
# getCDROMmedia
```

This will list a virtual CD-ROM media devices with the exact device name.

Example output:

```
[root@ixpl977-1a ~]# getCDROMmedia  
HP Virtual DVD-ROM:scd0
```

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

12.2 Configure and Verify ILO Connection

Note: For latest procedure to configure iLO, please refer platform configuration guide [1]

This procedure is applicable to all HP.

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

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

Minimal steps are:

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

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

1. Open Internet Explorer on a workstation and enter in the ILO IP address.
2. You will get a SSL security warning
3. Accept the warning.
4. Once you are logged in click on Launch to start **Integrated Remote Console**
5. If you will receive another certificate warning click on **Yes** to continue
6. If you get the application's digital signature can not be verified click Always trust content from this publisher then click **Run**.
7. A remote console window will now appear to allow you to access the HP server.

12.3 Adding ISO Images to the PM&C Image Repository

Note: For latest procedure to Add ISO image to PM&C please refer platform configuration guide [1]

This procedure will provide the steps how add ISO images to PM&C repository.

IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

1. Make the image available to PM&C

There are two ways to make an image available to PM&C:

- Insert the CD containing an iso image into the removable media drive of the PM&C server.
- Use sftp to transfer the iso image to the PM&C server in the/
var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
 - Go into the directory where your ISO image is located (not on the PM&C server)
 - Using sftp, connect to the PM&C management server


```
> sftp pmacftpusr@<PM&C_management_network_IP>
> put <image>.iso
```
 - After the image transfer is 100% complete, close the connection


```
> quit
```

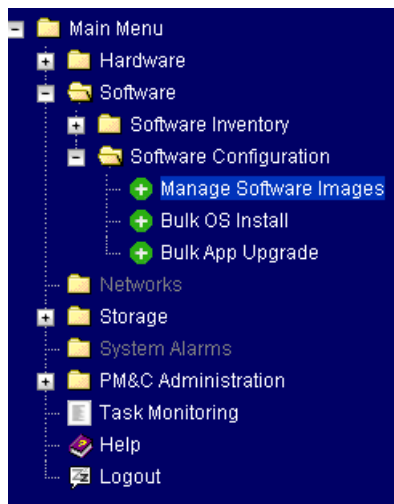
Note: Refer to the documentation provided by application for pmacftpusr password.

2. PM&C GUI: Login

- Open web browser and enter:
`http://<management_network_ip>/gui`
- Login as pmacadmin user

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

Navigate to Main Menu ⌚ Software ⌚ Software Configuration ⌚ Manage Software Images



4. PM&C GUI:Add image

- Press the **Add Image** button.



- Use the dropdown to select the image you want to add to the repository.
Note: Optical media device appears as device: `//dev/hdc`
- Add appropriate image description and press **Add New Image** button.

Note:

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

Image Search Path:

/var/TKLC/upgrade/*.iso

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

/var/TKLC/upgrade/872-2173-101-3.1.0_31.5.0-i386.iso

/var/TKLC/upgrade/872-2173-101-3.1.0_31.5.0-i386.iso

/var/TKLC/smac/image/isoimages/home/smacftpusr/872-2173-101-3.1.0_31.5.0-i386.iso

device://dew/hdc

Add New Image

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

12.4 How to remove IP Address and Route

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

- Remove IP address

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

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

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

- Remove IP route

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

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

Where **{gw_ipaddress}** will be the IP address of the gateway needs to be removed, e.g 172.21.48.250

Where **{net_ipaddress}** will be the IP address of network, e.g 172.20.48.0

Where **{net_mask}** will be the mask of network, e.g 255.255.254.0

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

12.5 How to recover OA board password

Note: For latest procedure to recover OA board password please refer platform configuration guide [1]

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

- Connect a serial console on the OA RJ45 port
- Open a console using putty or Hyper Terminal
- Press the OA reset button during 5s
- While the OA restart press "L" to enter in the Lost password mode.

5. Finally password should be displayed

12.6 Granting and revoking DBA role to NSP user

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

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

```
# su - oracle
```

2. Login to sqlplus console using command:

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

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

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

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

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

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

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

```
Revoke succeeded.
```

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

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

If the result of above command is not the same as shown above and still contains DBA role in result set then please contact Oracle Support AppendixA. **My Oracle Support (MOS)**

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

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

```
# su - oracle
```

2. Login to sqlplus console using command:

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

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

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

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

If the output of command is same as show above then execute below steps to grant DBA role to NSP user but if DBA role is shown in the above list then skip the execution of below steps.

4. Execute command to grant the DBA privilege to NSP user

```
# GRANT DBA TO NSP;
```

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

```
Grant succeeded.
```

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

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

```
GRANTED_ROLE
```

```
-----
```

```
RESOURCE  
CONNECT  
DBA
```

If the result of above command is not the same as shown above and still does not show DBA role in the result set then please contact Oracle Support, AppendixA. **My Oracle Support (MOS)**

AppendixA. My Oracle Support (MOS)

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

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

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

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

MOS is available 24 hours a day, 7 days a week, 365 days a year.

AppendixB. Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at <http://docs.oracle.com>.
2. Under Industries, click the link for Oracle Communications documentation.

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

3. Click Oracle Communications Documentation for Tekelec Products.
4. Navigate to your Product and then the Release Number, and click the View link (the Download link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select Save Target As.