

**Oracle® Communications
Performance Intelligence Center
Installation Guide
Release 10.1.5
E56065 Revision 1**

August 2015

Oracle Communications Performance Intelligence Center Installation Guide, Release 10.1.5

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 Section 16 for instructions on accessing My Oracle Support.

TABLE OF CONTENTS

TABLE OF CONTENTS	3
LIST OF FIGURES	6
LIST OF TABLES	6
1 INTRODUCTION.....	7
1.1 Document Admonishments.....	7
1.2 Reference Documents.....	7
1.3 Related Publications.....	7
1.4 Documentation Availability, Packaging and Updates	7
1.5 Scope And Audience	8
1.6 Requirements and Prerequisites.....	8
1.6.1 Hardware Requirements	8
1.6.2 Software Requirements	8
2 INSTALLATION OVERVIEW.....	9
2.1 Flowchart Description	9
2.2 PIC High Level Manufacturing	10
2.3 Data Record Storage.....	11
2.4 Management Server	12
2.5 Integrated/Probed Acquisition SubSystem.....	12
2.6 Mediation SubSystem.....	14
3 SYSTEM CONFIGURATION ON TPD HARDWARE	15
3.1 Operating system installation.....	15
4 SYSTEM CONFIGURATION ON ODA	16
4.1 OS Installation.....	16
4.1.1 Configure Network	16
4.2 ODA_BASE Template Deployment	16
4.3 Creation of Database.....	16
4.3.1 Creation of DWS database using oakcli	17
4.3.2 Creation of Management Server database using oakcli	18
4.4 MEDIATION user and Tablespace creation.....	19
4.4.1 REDO log and UNDO tablespace configuration	19
4.4.2 Procedure to create IXP user and tablespaces	21
4.4.3 Procedure to Disable Archive Log	22
4.5 Management Server user and Tablespace creation.....	22
4.6 Create Weblogic VMs.....	23
5 SYSTEM CONFIGURATION ON ZFS	25
5.1 ZFS server Installtion.....	25
5.2 Configure ZFS.....	25
6 MANAGEMENT SERVER APPLICATION INSTALLATION PROCEDURES ON ODA 26	
6.1 Management Server Pre-Install Configuration	26
6.1.1 Domain directory verification.....	26
6.1.2 Enable Clear Text setting on weblogic console	26
6.1.3 Update parameters for datasources on weblogic console.....	26

6.1.4	Tune memory parameters on weblogic console	26
6.1.5	Disable Clear Text setting on weblogic console	26
6.1.6	Change nsp user password in database	27
6.1.7	Stop Managed Servers	27
6.1.8	Start Managed Servers	27
6.1.9	Start Node Manager.....	27
6.1.10	Pre-Install steps on Admin Server	28
6.1.11	Verify key exchange between Admin and MS1,MS2,Oracle server.	28
6.1.12	Pre-Install steps on MS1 and MS2 server	28
6.1.13	Pre-install steps on Oracle server.....	28
6.2	Management server application installation	29
6.2.1	Mount Management Server media.....	29
6.2.2	Install Management Server	29
6.3	Management Server Post Installation Configuration	29
6.3.1	Restart Weblogic Servers	29
6.3.2	Configure firewall and permissions on Admin server and copy required files to respective server.	30
6.3.3	Change the open file limit and configure firewall on MS1 and MS2 servers	31
6.3.4	Create directory structure and key sharing on Oracle server	31
6.3.5	Configure NFS server	32
6.3.6	Schedule Management database backup job on oracle server.....	32
6.3.7	Change Customer Icon (Optional)	32
6.3.8	Install Optional Applications.....	33
6.3.9	Configure Purchased Tokens	33
6.3.10	Configure Open file limit for OTD (Mandatory)	34
6.3.11	Configure Weblogic Plug-In (Mandatory).....	34
6.4	Management Server Post Install Health Check.....	34
7	ACQUISITION SERVER APPLICATION INSTALLATION PROCEDURES.....	35
7.1	Pre-Install Configuration	35
7.1.1	Temporary customer IP assignment.....	35
7.1.2	Copy ISO.....	35
7.1.3	Configure server.....	35
7.2	Acquisition Server Pre-Install Healthcheck	36
7.3	Install Acquisition Server Application	36
7.4	Configure Site and Subsystem for Acquisition Server	37
7.5	Acquisition Server Healthcheck post customer integration.....	37
8	DATA RECORD STORAGE INSTALLATION PROCEDURES.....	41
8.1	Configure Data Record Storage on ODA	41
8.2	Configure Oracle on ODA based Data Record Storage	41
8.3	Add Data Record Storage to CCM.....	42
9	MEDIATION APPLICATION INSTALLATION PROCEDURES	44
9.1	Mediation Server Pre-Install Configuration	44
9.1.1	Verify each server healthcheck.....	44
9.1.2	Configure Bonding Interface (Optional).....	45
9.1.3	Create the bulkconfig file	45
9.1.4	Configure the server hostname.....	45
9.2	Install Mediation Server	45
9.2.1	Temporary customer IP assignment.....	46
9.2.2	Copy ISO.....	46
9.2.3	Install the application.....	46
9.2.4	Analyze the installation log	46
9.3	Mediation Server Post-Install Healthcheck	46

PIC 10.1.5 Installation Guide

9.4 Integrate Customer Network.....	48
9.5 Add Mediation Subsystem to CCM	49
9.6 Install xDR Builders	50
9.7 Capacity Management KPIs installation.....	51
9.7.1 Installation Procedures for Capacity Management standard KPIs	51
9.8 Mediation Subsystem Healthcheck.....	52
9.9 Mediation Server Post-Integration Configuration (Optional).....	58
9.9.1 CSV streaming feeds and DataBroker.....	58
9.9.2 Delivery Network Failure and Recovery (DataBroker).....	59
10 APPENDIX: MANUAL CONFIGURATION OF ETHERNET INTERFACES	61
11 APPENDIX: PIC BULKCONFIG FILE DESCRIPTION	75
11.1 Management Server Bulkconfig File Description	75
11.2 Mediation Server Bulkconfig File Description	78
11.3 DWS Bulkconfig File Description.....	83
11.4 Acquisition Server Bulkconfig File Description.....	87
12 APPENDIX: SWITCHES CONFIGURATION	93
13 APPENDIX: CAPACITY MANAGEMENT PROTRAQ CONFIGURATIONS	94
14 APPENDIX: HOW TO CONFIGURE NTP.....	98
14.1 NTP architecture	98
14.2 Check the NTP precision.....	98
15 APPENDIX: NETWORK PORTS BETWEEN PIC COMPONENTS	99
16 APPENDIX: MY ORACLE SUPPORT (MOS).....	100
17 APPENDIX: LOCATE PRODUCT DOCUMENTATION ON THE ORACLE TECHNOLOGY NETWORK SITE.....	101
18 APPENDIX: HOW TO ACCESS CONSOLE OF VM IN ODA	102

List of Figures

Figure 1. Flowchart conventions..... 9
Figure 2. High level installation..... 10
Figure 3. Data Record Storage installation on ODA server..... 11
Figure 4. Mangement server installation on ODA 12
Figure 5. Integrated and Probed Acquisition SubSystem Installation 13
Figure 6. Mediation subsystem installation 14

List of Tables

Table 1. Admonishments 7

1 INTRODUCTION

1.1 Document Admonishments

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

Table 1. Admonishments

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

1.2 Reference Documents

- [1] [Platform 7.0 Configuration Procedure References](#) E53486, December 2014
- [2] [TPD Initial Product Manufacturing](#) E53017, December 2014
- [3] [HP Solutions Firmware Upgrade Pack 2.2.8](#), E59723, March 2015
- [4] [Oracle Firmware Upgrade Pack](#), E54964, June 2014
- [5] [ODA Getting Started Guide](#), E22692-41, February 2015
- [6] [Weblogic On ODA](#), E52728, May 2014
- [7] [Oracle Database Appliance - 12.1.2 and 2.X Supported ODA Versions & Known Issues \(Doc ID 888888.1\)](#)
- [8] [ZFS Storage Appliance Installation Guide](#), E55847-01, December 2014
- [9] [ZFS Storage Appliance Administration Guide](#), E55851-01, December 2014
- [10] [OTD Administration Guide](#), E23389_01
- [11] [Tekelec OTN](#)
- [12] [PIC 10.1.5 Maintenance Guide](#), E56062
- [13] Teklec Default Passwords ,TR006061
- [14] [PIC Hardware installation Guidelines](#), E64544
- [15] [PIC Data Warehouse Server \(DWS\) on HP DL380 Gen 9 Installation](#), Doc ID 2028670.1
- [16] [PIC Packet Data Unit Storage \(PDU\) Server on HP DL380 Gen 9 Installation](#), Doc ID 2034894.1

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 and is also published as a separate document on the Oracle Technology Network Site.

1.4 Documentation Availability, Packaging and Updates

Oracle provides documentation with each system and in accordance with contractual agreements. For General Availability (GA) releases, the documentation can be downloaded from [OTN](#).

The Oracle PIC 10.1.5 documentation set is released on Management Server iso.

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

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

1.5 Scope And Audience

This document describes the procedures to install a PIC system at Release 10.1.5.

This document is intended for use by trained engineers in software installation on both SUN and HP hardware. A working-level understanding of Linux and command line interface is expected to successfully use this document.

It is strongly recommended that prior to performing an installation of the operating system and applications software, on either a HP or ODA system, the user read through this document.

Note: The procedures in this document are not necessarily in a sequential order. There are flow diagrams in the Installation Overview 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 installing the PIC system should reference these flow diagrams during this installation process.

1.6 Requirements and Prerequisites

1.6.1 Hardware Requirements

Refer [PIC Hardware Guidelines](#)

1.6.2 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 Probed and Integration
- TADAPT
- TPD

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 produce files corresponding to 11G and Weblogic 10.3.6 must be downloaded and used in the installation. The patch set is already mentioned in the ODA documentation(s) [ODA](#) and [Weblogic on ODA](#)

2 INSTALLATION OVERVIEW

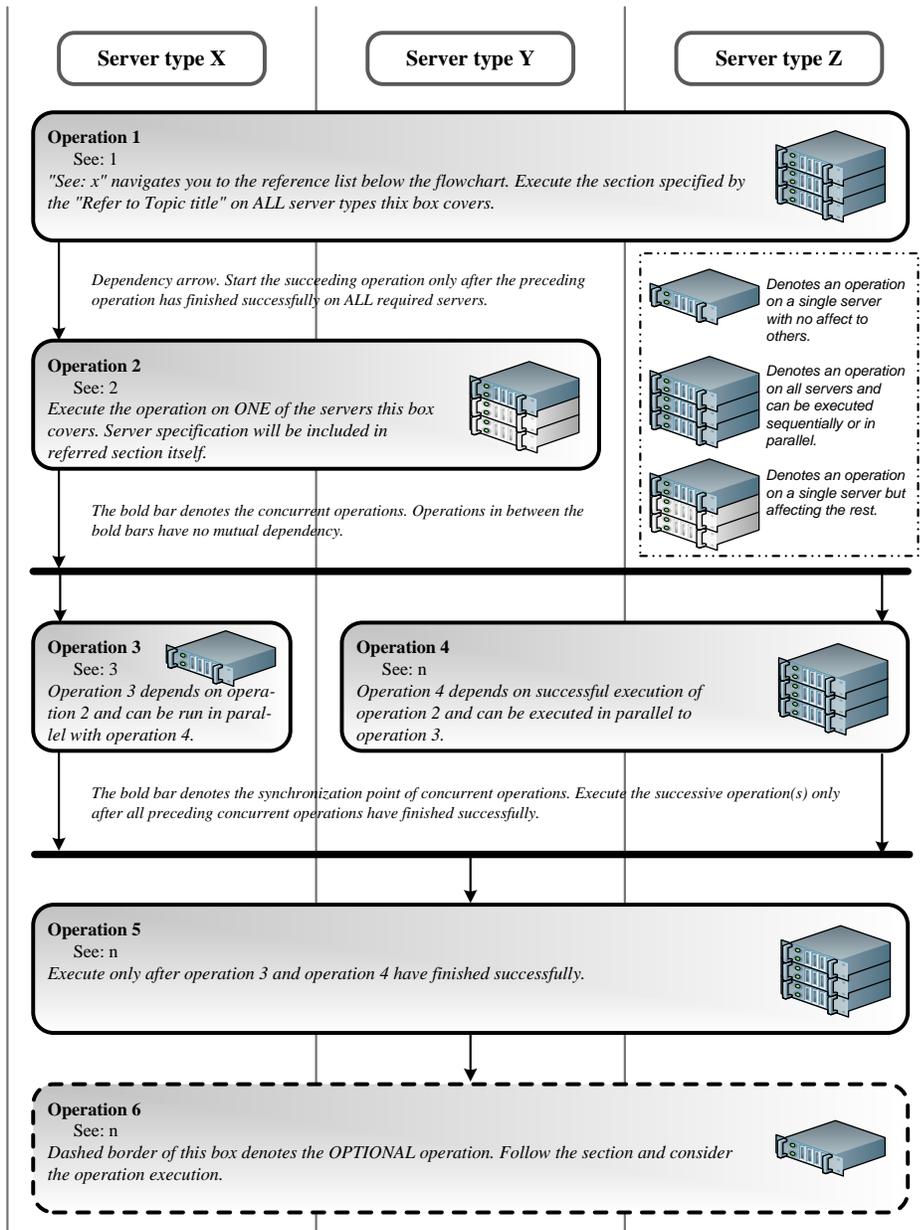
This section provides installation overview information for the PIC 10.1.5 system by using flowcharts that depict the sequence of procedures for each subsystem and their associated servers.

2.1 Flowchart Description

The flowcharts within each section depict the sequence of procedures that need to be executed to install the specified subsystem. Here the servers can be physical machines or virtual machines (on ODA)

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

Figure 1. Flowchart conventions



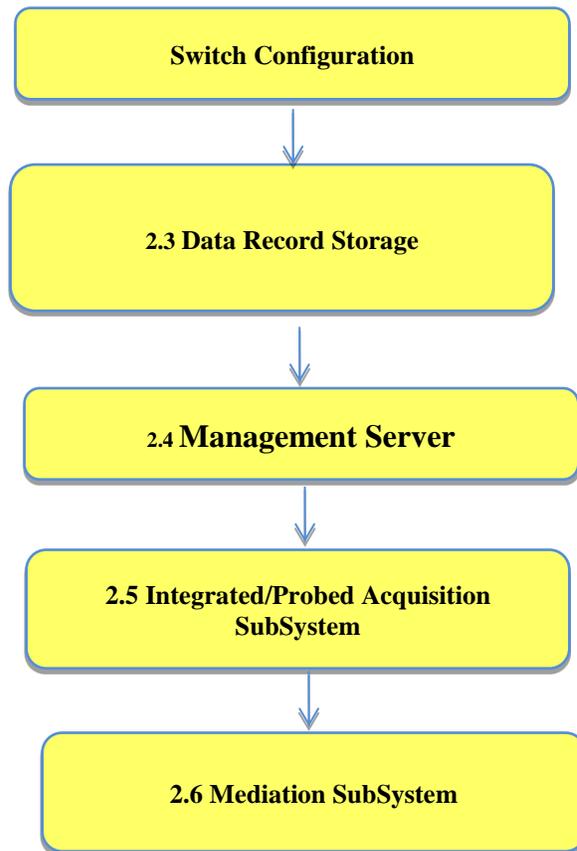
2.2 PIC High Level Manufacturing

This flowchart describes PIC high-level manufacturing installation overview.

Mediation/Management/Data Record Storage/Acquisition components can be installed in parallel, however the integration of the PIC components require that management server is already present. Therefore it is recommended to follow the sequence depicted in below flow chart. Referring to graphic below, the hardware applicable to each component is identified and for each component, the applicable flowchart is identified by section of this document where it is located.

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

Figure 2. High level installation



Note: PIC installation may require the following to be completed before proceeding with installation:

1. Firmware Upgrade, Refer [HP Firmware Upgrade](#) and [ORACLE Firmware Upgrade](#)

2.3 Data Record Storage

This flowchart depicts the sequence of procedures that must be executed to install the data record storage on ODA. The OS installation must be done on both physical nodes on ODA.

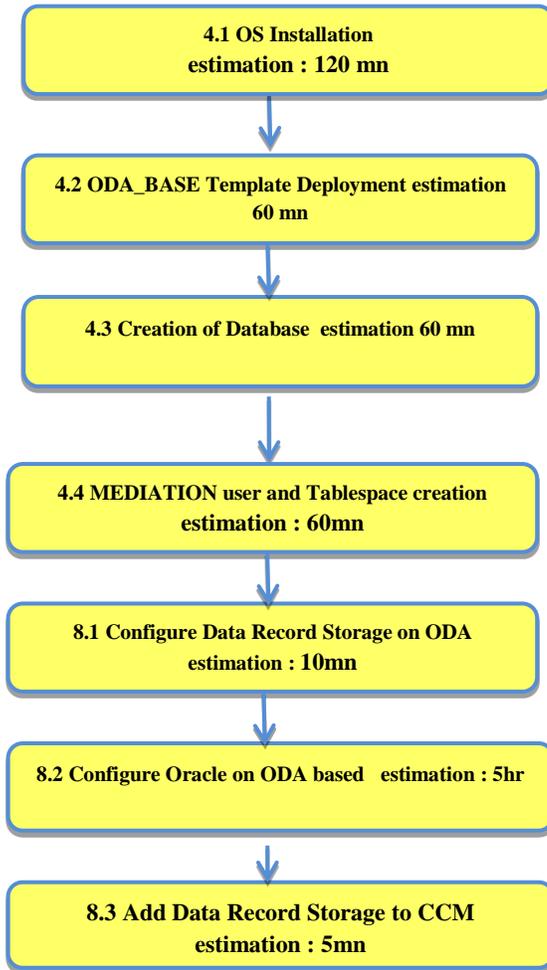


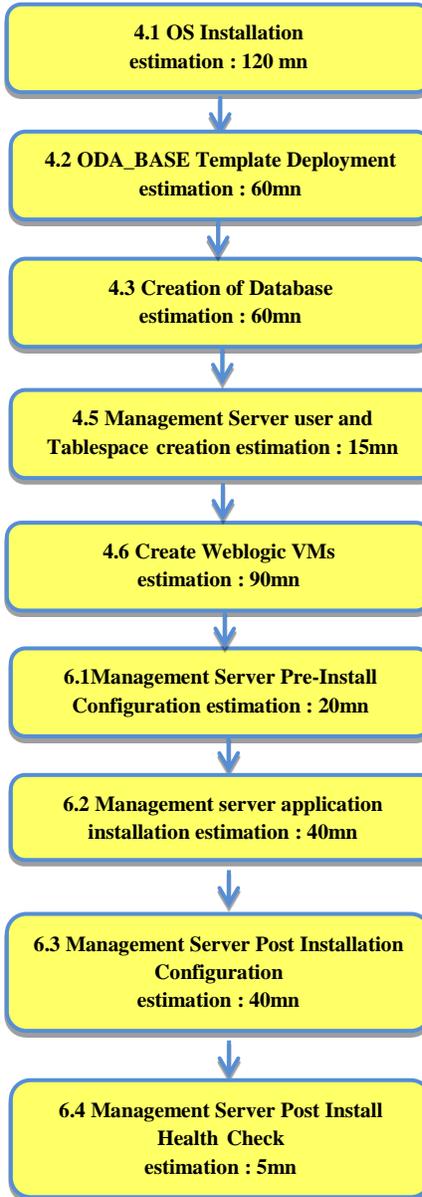
Figure 3. Data Record Storage installation on ODA server

Note: In the case where ODA is shared between DWS and management server, there is no need to perform 4.1 and 4.2 if these steps are already performed.

2.4 Management Server

This flowchart depicts the sequence of procedures that must be executed to install the Management server on ODA. OS installation must be done on both the physical nodes on ODA.

Figure 4. Management server installation on ODA



Note: In the case where ODA is shared between management server and DWS, there is no need to perform 4.1 and 4.2 if these steps are already performed.

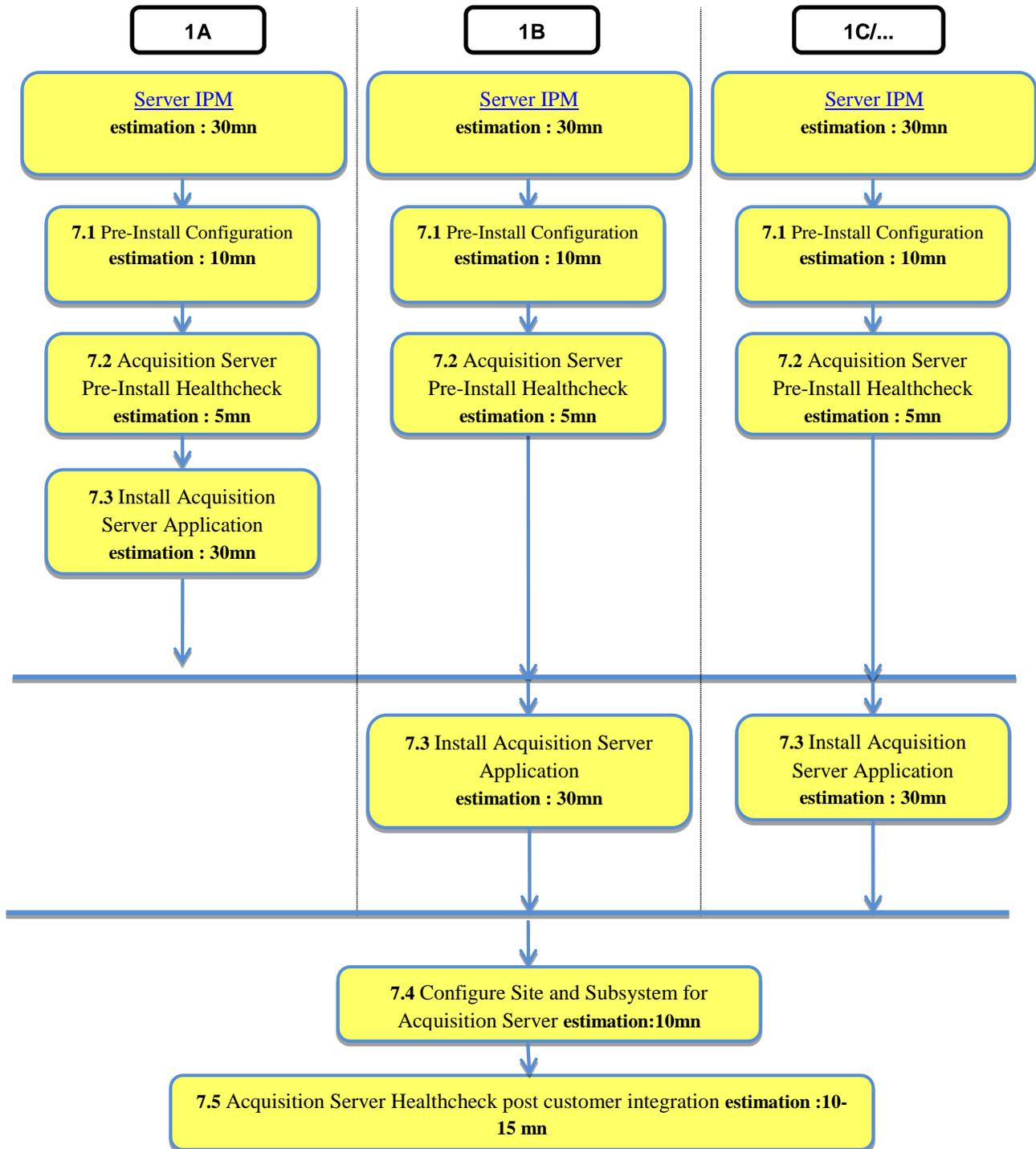
2.5 Integrated/Probed Acquisition SubSystem

This flowchart depicts the sequence of procedures that must be executed to install the integrated/probed acquisition subsystem and associated servers.

PIC 10.1.5 Installation Guide

- IPM sequence is not required for E5-APP-B as E5-APP-B card is provided with already installed TPD.
- For Probed acquisition the installation is always done on the stand alone server.

Figure 5. Integrated and Probed Acquisition SubSystem Installation

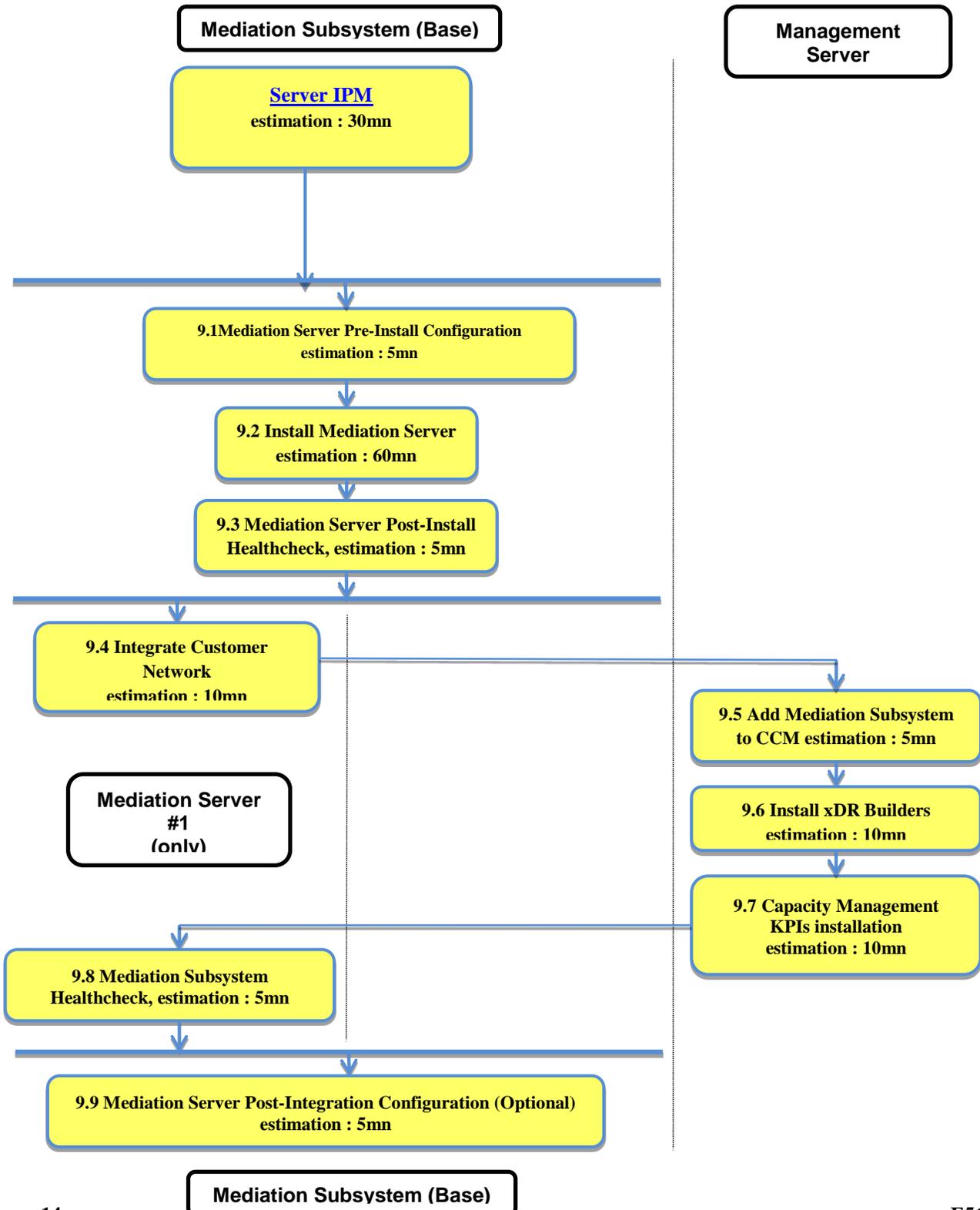


2.6 Mediation SubSystem

This flowchart depicts the sequence of procedures that must be executed to install the mediation subsystem and associated servers. The Mediation subsystem consists of the following types of servers:

- Mediation Base server

Figure 6. Mediation subsystem installation



3 SYSTEM CONFIGURATION ON TPD HARDWARE

This section provides instructions for installing the operating system on the TPD servers, and doing some basic configuration before installing applications.

3.1 Operating system installation

Please follow instructions for OS installation from [Platform 7.0 IPM Procedures](#).

Supported TPD Hardware	Recommended Command	Comments
HP G6	TPDnoraid console=tty0	
HP Gen8	TPDnoraid console=tty0	
HP Gen9	TPDnoraid console=tty0	
X5-2	TPDnoraid console=tty0	
E5-APP-B	TPDlvm	Only to use if manufacturing has IPMed E5-APP-B card using TPD 5.5.1 instead of TPD 7.0.2

4 SYSTEM CONFIGURATION ON ODA

This section provides the procedures for initializing the ODA in case of ODA hardware. The general installation and administration instructions have been provided in http://docs.oracle.com/cd/E22693_01/doc.12/e22692/toc.htm.

4.1 OS Installation

ODA must be installed (OS installation) with virtualized image support. Please refer document <https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1520579.1> for the OS installation in virtual platform mode. The user can follow the “Step by Step Instructions” link to perform the OS installation with virtualized platform support.

Warning: The fully qualified hostnames on ODA VMs must not exceed 30 characters. The fully qualified name is the machine name appended by domain name, for example “oda-ent-mlh1.fr.oracle.com”, here “oda-ent-mlh1” is the name given to the machine and “fr.oracle.com” is the domain name. Care must be taken while defining domain name and machine host name to ensure above limit is respected.

4.1.1 Configure Network

Configuring network on dom0 for both nodes. Refer the steps in http://docs.oracle.com/cd/E22693_01/doc.12/e22692/predeploy.htm#CMTIG298

4.2 ODA_BASE Template Deployment

This refers to creating the ODA_BASE VM on both the nodes. Please refer steps in http://docs.oracle.com/cd/E22693_01/doc.12/e22692/deploy.htm#CMTIG142

Recommendations:

- a) Select 12 cores of CPU and 192 GB of RAM
- b) PIC does not need any additional VLANs, so creation of additional VLANs can be skipped

Note: It is recommended to apply the following patch in ODA 2.10 After the ODA_BASE Deployment.

Oracle Support Document 1929576.1 (ODA ODAVP Created Shared Repositories with VM Clones are Missing / Gone on both DOM0 DOM1 Nodes in /OVS on 2.10 using non-lowercase Node Names) can be found at: <https://support.oracle.com/epmos/faces/DocumentDisplay?id=1929576.1>

If the above patch is applied after the Management Server installation then it is recommended to restart the nspservice, after applying the patch.

4.3 Creation of Database

Note: Only one database can be created using Oracle database manager configurator. Either create DWS database or Management database by following recommendations as mentioned below. If one database has been created using configurator then another database will be created using oakcli command line utility as explained in section 4.3.1 and 4.3.2 for DWS and management server respectively.

This refers to the creation of the Oracle database server on the ODA_BASE. Please refer the steps in http://docs.oracle.com/cd/E22693_01/doc.12/e22692/deploy.htm#CMTIG142

Requirement:

- a) Database Deployment: Oracle Enterprise Edition 11g

Recommendations for DWS:

- a) Database Name: IXP

PIC 10.1.5 Installation Guide

- b) DB Block Size : 16834 bytes
- c) Database Backup: External Backup
- d) Disk Group Redundancy: Normal
- e) Database Class: Large Database (SGA 24GB, 6 CPU cores)
- f) Database Language: American
- g) Database Charset: AL32UTF8
- h) Configure DB Console : Yes
- i) “/cloudfs” partition with default size (50GB)
- j) Database Type: Default (OLTP)

Recommendations for Management Server:

- a) Database Name: NSP
- b) DB Block Size : 8192 bytes
- c) Database Backup: External Backup
- d) Disk Group Redundancy: Normal
- e) Database Class: Small Database
- f) Database Language: American
- g) Database Charset: AL32UTF8
- h) Configure DB Console : Yes
- i) “/cloudfs” partition with default size (50GB)
- j) Database Type: Default (OLTP)

Note: The partition “ /cloudfs” can be used for the external storage either for example PDU storage for small PIC system using NFSv4. The size of this partition must be provided keeping external storage usage point in mind.

4.3.1 Creation of DWS database using oakcli

Note: Please see the recommendations in sec 4.3 before creating the database.

The steps mentioned in section 4.3.1 are applicable only if mediation server database is not created during the ODA_BASE deployment. The steps are especially useful for small system, where many database are needed.

- a) Log on to oracle box as root user and run following command from home directory of root user:

```
# oakcli show databases
```

Similar kind of output will be shown on the screen:

```
[root@oda-ent-mlh1 ~]# oakcli show databases
DatabaseName DatabaseType DatabaseHomeName DatabaseHomeLocation DatabaseVersion
-----
NSP SINGLE OraDb11204_home3 /u01/app/oracle/product/11.2.0.4/dbhome_3 11.2.0.4.2(18031668,18031740)
```

It should show the database list. If the database IXP doesn't exist, then create database as mentioned in next step.

- b) DWS requires Oracle 11g Enterprise Edition, large database with Database Block Size 16384 bytes. There is no constraint on database name, however it is recommended to use “IXP” as the DWS database name:

Creating the database using command line takes default Database Block Size of 8192 bytes. To create a database having Database Block Size of 16384 bytes requires a custom response file. The custom response file can be created using the following command:

```
# oakcli create db_config_params -conf <response_file_name>
```

Follow the following example.

```
[root@oda-ent-mlh1 ~]# oakcli create db_config_params -conf rsFileForDWS
Please select one of the following for Database Block Size [1 .. 4]:
1 => 4096
2 => 8192
3 => 16384
4 => 32768
3
Selected value is: 16384

Specify the Database Language (1. AMERICAN 2. Others) [1]:1
Selected value is: AMERICAN

Specify the Database Characterset (1. AL32UTF8 2. Others) [1]:1
Selected value is: AL32UTF8

Specify the Database Territory (1. AMERICA 2. Others) [1]:1
Selected value is: AMERICA

Specify the Component Language (1. en 2. Others) [1]:1
Selected value is: en

Successfully generated the Database parameter file 'rsFileForDWS'
[root@oda-ent-mlh1 ~]#
```

- c) After creating the response file **create Enterprise Edition, large database with external storage and normal redundancy** with following command:

```
# oakcli create database -db <db_name> -params <response_file_name>
```

Where, <db_name> is the name of database “IXP” and <response_file_name> is the name of response file created in the previous step.

Select the node to create database as node 1.

Provide the password same as default root user password on ODA whenever it prompts for password.

4.3.2 Creation of Management Server database using oakcli

Note: Please see the recommendations in section 4.3 before creating the database.

The steps mentioned in section 4.3.2 are applicable only if management server database is not created during the ODA_BASE deployment. The steps are especially useful for small system deployment, where many database are needed.

- a) Log on to oracle box as root user and run following command:

```
# oakcli show databases
```

Similar kind of output will be shown on the screen:

```
[root@oda-ent-mlh1 ~]# oakcli show databases
DatabaseName DatabaseType DatabaseHomeName DatabaseHomeLocation DatabaseVersion
-----
IXP SINGLE OraDb11204_home3 /u01/app/oracle/product/11.2.0.4/dbhome_3 11.2.0.4.2(18031668,18031740)
```

PIC 10.1.5 Installation Guide

It should show the database list. If the database NSP doesn't exist, then create database as mentioned in next step.

- b) Management Server database requires Oracle 11g Enterprise Edition, small database with Database Block Size 8192 bytes. It is required to use "NSP" as database name:

Creating the database using command line takes default Database Block Size of 8192 bytes.

```
# oakcli create database -db <db_name>
```

Where, <db_name> is the name of database "NSP"

When it prompts, select **Enterprise Edition, Others (small)**.

Select the node to create database as node 1.

Provide the password same as default root user password on ODA whenever it prompts for password.

4.4 MEDIATION user and Tablespace creation

Perform below procedures only if IXP user and tablespaces don't exist. In case they exist don't perform below steps and move directly to section 4.5.

4.4.1 REDO log and UNDO tablespace configuration

Note: Before creation of user and tablespaces make sure the REDO logs and UNDO tablespace are available with following recommendations:

1. REDO Logs: 4 REDO log file size of 20 GB each.
2. UNDO tablespace: 4 files with maximum size of the file 64GB auto extending by 5 MB.

4.4.1.1 Configure REDO logs

REDO Logs: 4 REDO log file size of 20 GB each. If not then execute following procedure :

1. Log into the database as SYS user.

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

```
2. sql> SELECT GROUP#, BYTES, STATUS from v$log;
```

The above command lists the REDO log groups number, size(in bytes) and status. Check the groups and size of log files. If the size of the log file is less than 20G then it should be replaced with a new logfile of size 20G. If the count of logfile is less than 4 then additional logfile should be created.

- A redo log file size cannot be altered.
- Also, At any time there should be minimum of 2 REDO log files present in the database.
- If there exists 2 REDO logfile and one is to be dropped then create a new logfile and then delete the existing one(i.e. we just cannot delete all the existing REDO log file and create new).
- A REDO log file with status 'ACTIVE' or 'CURRENT' cannot be deleted.
- To delete a logfile with status 'CURRENT', first switch to another log file.
- To delete a logfile with status 'ACTIVE' change the status of the logfiles to 'INACTIVE'.

3. Following command Switch between log files and changes their status

```
sql> ALTER SYSTEM SWITCH LOGFILE;
```

In large database on ODA server there are by default 3 log groups(1, 2 and 3) of size 4G each. Keep switching between the log files with above provided command till the status of log group 1 becomes 'CURRENT';

4. After log group status becomes 'CURRENT', if the status of the log groups 3 is not 'INACTIVE' then issue following command:

```
sql> ALTER SYSTEM CHECKPOINT;
```

5. Delete the log group 3 with following command:

```
sql> ALTER DATABASE DROP LOGFILE GROUP 3;
```

6. Recreate log group 3 with increased size with following command:

```
sql> ALTER DATABASE ADD LOGFILE GROUP 3 SIZE 20G;
```

7. Create another log group 4 using following command:

```
sql> ALTER DATABASE ADD LOGFILE GROUP 4 SIZE 20G;
```

8. Make log group 3 or 4 current by switching between the log files with command in **step3** till the status of any of log group 3 or 4 becomes 'CURRENT'.

9. After switching to log group 3 or 4, if the status of the log groups 1 and 2 is not 'INACTIVE' then issue following command:

```
sql> ALTER SYSTEM CHECKPOINT;
```

10. Delete the log groups 1 and 2 with following command:

```
sql> ALTER DATABASE DROP LOGFILE GROUP 1;
sql> ALTER DATABASE DROP LOGFILE GROUP 2;
```

11. Recreate the log groups 1 and 2 with following command:

```
sql> ALTER DATABASE ADD LOGFILE GROUP 1 SIZE 20G;
sql> ALTER DATABASE ADD LOGFILE GROUP 2 SIZE 20G;
```

4.4.1.2 Configure datafile in UNDO tablespace

For a large database, It is suggested to have 4 datafiles of size 50GB each extendable upto 64GB auto extending by 5 MB. On ODA the datafile size can be maximum upto 65535MB, which is 1MB less than 64 GB. If not then execute following procedure.

PIC 10.1.5 Installation Guide

1. Log into the database as SYS user.

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

2. List the datafiles in UNDO tablespace using following command:

```
sql> select FILE_NAME, AUTOEXTENSIBLE, MAXBYTES, MAXBLOCKS, INCREMENT_BY
from dba_data_files where TABLESPACE_NAME like 'UNDO%';
```

Verify the number of datafiles in UNDO tablespace and their size from the output of above command.

If the MAXBYTES is less than 65535MB then use the following command to alter the size:

```
sql> ALTER DATABASE DATAFILE <UNDO_datafile_name> AUTOEXTEND ON NEXT 5M
MAXSIZE 65535M;
```

where, <UNDO_datafile_name> is the name of datafile which is to be altered.

Example:

```
sql> ALTER DATABASE DATAFILE '+DATA/ixp/datafile/undotbs1.258.874104679'
AUTOEXTEND ON NEXT 5M MAXSIZE 65535M;
```

3. Create more datafiles in UNDO tablespace by issuing following command:

```
sql> ALTER TABLESPACE "UNDOTBS1" ADD DATAFILE '+DATA' SIZE 50G REUSE
AUTOEXTEND ON NEXT 5M MAXSIZE 65535M;
```

Note: The creation of datafile of size 50GB takes around 5-6 mins. The above procedure may take upto 30 min to complete.

4.4.2 Procedure to create IXP user and tablespaces

1. Copy MEDIATION iso to "/cloudfs" directory on oracle box and log on as root user.
2. Mount the MEDIATION iso to /mnt/upgrade. If directory does not exists then create it by below command:

```
# mkdir -p /mnt/upgrade
# mount -o loop <ISO PATH> /mnt/upgrade
```

3. Change user to oracle and export ORACLE_SID variable

```
# su - oracle
# export ORACLE_SID=IXP
# ORAENV_ASK=NO source oraenv
```

4. Execute script createUserTbsp.sh

```
# cd /mnt/upgrade/migration/oracle/instance/cmd/
# ./createUserTbsp.sh <SYS_CONNECTION_STRING>
```

Where, <SYS_CONNECTION_STRING> is in format SYS/<SYS_password> and <SYS_password> is System password, which should be same as "*****"

Note: In logs there will be many spool log error which should be ignored. Verify the logs for errors other than spool log error

5. Switch to root user and umount the ISO after successful execution of above step 4 using command

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

4.4.3 Procedure to Disable Archive Log

1. Login as sysdba user

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

2. Shutdown database

```
sql> shutdown immediate;
```

3. Start database

```
sql> startup mount;
```

4. Disable archive log

```
sql> alter database noarchivelog;
```

5. Open database

```
sql> alter database open;
sql> quit;
```

4.5 Management Server user and Tablespace creation

Note: Please perform below steps only if NSP user and tablespaces don't exist. In case they exist don't perform below steps.

1. Copy Management Server iso to "/cloudfs" directory on oracle box and log on as root user.
2. Mount the Management Server iso to /mnt/upgrade. If directory does not exist then create it by below command:

```
# mkdir -p /mnt/upgrade
# mount -o loop <ISO PATH> /mnt/upgrade
```

3. Change user to oracle and export ORAENV_ASK and ORACLE_SID variables

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

4. Execute create_tablespaces_user_ODA.sql to create user and table space.

```
sql> @/mnt/upgrade/scripts/create_tablespaces_user_ODA.sql $ORACLE_HOME
It will prompt password for nsp user, enter "default password used for root user".
```

5. Set Global Names to false:

```
sqlplus / as sysdba
sql> ALTER SYSTEM SET GLOBAL_NAMES=FALSE;
```

6. Disable Archive Log

- a) Shutdown database

```
sql> shutdown immediate;
```

- b) Start database

```
sql> startup mount;
```

PIC 10.1.5 Installation Guide

- c) Disable archive log

```
sql> alter database noarchivelog;
```

- d) Open database

```
sql> alter database open;  
sql> quit;
```

7. Umount the iso after successful execution of above steps using command

```
# su -  
# umount /mnt/upgrade
```

4.6 Create Weblogic VMs

Refer following URL in order to create weblogic VMs and OTD VMs

http://docs.oracle.com/cd/E52585_01/doc.29/e52728.pdf

Follow below mentioned recommendations while creating weblogic and OTD VMs

Limitation for Management Server hostname: Hostname must not be large as they are combined with domain name. Please ensure that machine name and domain name remains less than 30 characters.

General Information:

- a) Planned Deployment Cores: 10
- b) Provision Load balancer: Enable

Domains:

- c) Weblogic Version: 11g (10.3.6)
- d) Number of Domains: 1
- e) Domain Name: tekelec
- f) Number of Managed Servers: 2
- g) Number of Clusters: 1
- h) Cluster Sizing: 2
- i) Cluster: nsp
- j) Password: Enter default password used for root user
- k) JMS Distributed Destinations with DB Store: Enable
- l) JDBC Data Source: Enable

JMS Distributed Destinations:

- m) Service Name: NSP
- n) Database User Name: NSP
- o) Password: Enter default password used for root user

JDBC Data Source Configuration:

- p) Data Source Type: GenericDataSource
- q) JNDI Name: nspdatasource
- r) Service Name: NSP
- s) Database User Name: NSP

- t) Password: Enter default password used for root user
- u) Support Global Transactions: Enable

Load Balancer Information:

- v) Password: Enter default password used for root user
- w) OTD Port: 80

After providing all these input, user needs to save the configuration file. This configuration file can be reused later in case weblogic VMs are recreated if system crashes. Finish the configuration and wait for successful completion message.

5 SYSTEM CONFIGURATION ON ZFS

5.1 ZFS server Installation

Install the ZFS server using the documents described in (http://docs.oracle.com/cd/E56021_01/html/E55847/index.html)

5.2 Configure ZFS

This refers to the procedure for the network and storage configuration on ZFS after the ZFS server has been installed. The procedure shall also be needed to create the NFS shares. The procedures are available in (http://docs.oracle.com/cd/E56021_01/html/E55851/index.html)

The typical configuration required for creating the shares on ZFS server is mentioned below:

- a) Initial Appliance Configuration
- b) Network Configuration
- c) Storage Configuration
- d) Working with Shares

- a. Share Properties

During the creation of shared directories only the name and permissions should be provided. Permissions should be given to all, the name of the shared directory must contain the “pdu_”

Note: ZFS allows both nodes of the system to work in clustered mode (this mode has not been used during lab testing). Please, refer to the ZFS documentation to learn what are the advantages of using this mode and how to set it up: http://docs.oracle.com/cd/E56021_01/html/E55851/gokgf.html#scrolltoc.

Note: All the configuration should be done using BUI

Recommendation

- a) In general, multiple pools with same profile are discouraged for the following reasons:
 - i. Wastes system resources that could be shared in a single pool.
 - ii. Decreases overall performance.
 - iii. Increases administrative complexity.
 - iv. Log and cache devices can be enabled on a per-share basis.

Storage should be added to the existing pool with the same profile, unless the intent is to assign ownership of this resource to the cluster peer.

- b) As it is a good compromise between performance and high availability, even if usable disk space is reduced by a third of the overall disk space allocated, the “Double parity” data profile should be chosen; if usable disk space is not a priority, choose “Mirrored” as data profile (with the NSPF* option activated), in which case less than half of the allocated disk space can be used for PDU storage.
- c) The “Mirror log” should be chosen for the log profile (if possible select the profile where NSPF* is available).
- d) *NSPF indicates no single point of failure, which affords certain profiles the ability for a pool to survive through loss of a single disk shelf.

6 MANAGEMENT SERVER APPLICATION INSTALLATION PROCEDURES ON ODA

This section provides the procedures for installing the Management Server application.

6.1 Management Server Pre-Install Configuration

This procedure describes how to configure the Management servers, which is required prior to installing management server application.

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

6.1.1 Domain directory verification

1. Once all the weblogic VMs got created, log on to Admin weblogic VM and Managed servers weblogic VM as root user and verify “tekelec” directory inside /u01/ directory. If it is not there or empty then do not proceed ahead and contact Oracle Support, 16. APPENDIX: My Oracle Support (MOS)

Empty domain(tekelec) directory or non presence of domain directory depicts that there were some issues during weblogic VMs creation.

6.1.2 Enable Clear Text setting on weblogic console

1. Log on to Weblogic console and click on Lock & Edit button.
2. Select Domain Configurations > Domain > Security.
3. Expand the Advanced tab and check the Clear Text Credential Access Enabled property which is last in the list.
4. Click on save button and then Activate changes button.

6.1.3 Update parameters for datasources on weblogic console

1. Log on to Weblogic console and click on Lock & Edit button.
2. Select Services > Data Sources > nspdatasource > connection Pool.
3. Change the password to ‘nsp’ and update confirm password also.
4. Click on save button.
5. Select Services > Data Sources > wls_internal_ds > connection Pool
6. Change the IP in url with oracle box IP. For eg. **10.31.3.96**
7. Change the password to ‘nsp’ and update confirm password also.
8. Click on save button.
9. Click on Activate changes button.

6.1.4 Tune memory parameters on weblogic console

1. Log on to Weblogic console and click on Lock & Edit button.
2. Select Environment > Servers > ms1 > Server Start.
3. Change the values in Arguments to “ *-Xms2048m -Xmx2048m -XX:PermSize=128m -XX:MaxPermSize=1024m -Djava.net.preferIPv4Stack=true*”
4. Click on “Save” button.
5. Repeat step 2,3 and 4 for ms2 server also.
6. Click on save button and then Activate changes button.

6.1.5 Disable Clear Text setting on weblogic console

1. Log on to Weblogic console and click on Lock & Edit button.

PIC 10.1.5 Installation Guide

2. Select Domain Configurations > Domain > Security.
3. Expand the Advanced tab and uncheck the Clear Text Credential Access Enabled property which is last in the list.
4. Click on save button and then Activate changes button.

6.1.6 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 nsp;
# quit
```

4. Test password change is successful or not for nsp user.

```
# sqlplus nsp/nsp
```

5. If account locked then unlock account and execute step 4 again

```
# alter user nsp account unlock;
```

6. If above commands executes successfully you will get SQL prompt else repeat steps 1 to 5 again carefully.

```
# quit
```

6.1.7 Stop Managed Servers

Note : Do not execute if servers are already in failed or in not running state.

1. Log on to Weblogic console.
2. Select Environment > Servers > Control.
3. Select MS1 and MS2 servers using checkbox.
4. Select Shutdown > Force Shutdown Now
5. Wait until status of servers are shut_down/Force_shut_down [Task completed].

In case servers are not found in desired state, do not proceed ahead and contact Oracle Support, 16.
APPENDIX: My Oracle Support (MOS)

6.1.8 Start Managed Servers

1. Log on to Weblogic console.
2. Select Environment > Servers > Control.
3. Select MS1 and MS2 servers using checkbox.
4. Select Start and then select Yes.
5. Wait until status of servers are running and health is OK

In case servers are not found in desired state, do not proceed ahead and contact Oracle Support, 16.
APPENDIX: My Oracle Support (MOS)

6.1.9 Start Node Manager

1. Log on to Admin server and change user to oracle

```
# su - oracle
```

2. Start node manager by running below script

```
# sh /opt/oracle/middleware/wlserver_10.3/server/bin/startNodeManager.sh
```

3. Let this command be running on console. [Do not kill it]

Note: User must proceed further in installation with new putty session on Admin Server for rest of the steps. Application installation shall take care of the above started NodeManaged (in step 2).

Estimation time : Time taken for the application deployment, approx 30 mins.

6.1.10 Pre-Install steps on Admin Server

1. Log on to Admin server as root user.
2. Copy Management Server ISO from oracle server to admin server /u01/ directory and perform below steps

```
# mkdir -p /mnt/upgrade
# mount -o loop <ISO PATH> /mnt/upgrade
# sh /mnt/upgrade/scripts/nsp_pre_install_config.sh
```

Note: This script will prompt internal IP and passwords of MS1 and MS2 servers. Provide them very carefully. The internal IP address are assigned to eth0 interface on weblogic VMs.

6.1.11 Verify key exchange between Admin and MS1,MS2,Oracle server.

1. Log on to Admin server and change user to tekelec

```
# su - tekelec
# ssh -o StrictHostKeyChecking=no oracle@<DB_IP>
# exit
# ssh -o StrictHostKeyChecking=no oracle@< MS1_IP>
# exit
# ssh -o StrictHostKeyChecking=no oracle@< MS2_IP>
# exit
# exit
```

Note: Above commands should execute without any password.

6.1.12 Pre-Install steps on MS1 and MS2 server

1. Log on to ms1 server with root user.

```
# ln -s /u01 /opt/nsp
# mkdir -p /var/log/nsp /opt/www/nsp/resources/
# chown oracle:oinstall /var/log/nsp
# chown -R oracle:oinstall /opt/www
# chmod 777 /tmp
```

2. Repeat step 1 on ms2 server also.

6.1.13 Pre-install steps on Oracle server

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

```
# mkdir -p /var/log/nsp
# chown oracle:oinstall /var/log/nsp
# chmod 777 /var/log/nsp
# sed -i "/<Admin_IP>/d" /home/oracle/.ssh/known_hosts
```

Note: Admin_IP is Internal IP address of Admin server.

6.2 Management server application installation

This procedure describes how to install the management server Product on Admin server from the ISO.

Note: Run this procedure from VM console of Admin server. Refer [18_APPENDIX: How to access console of VM in oda](#) to access the VM console.

6.2.1 Mount Management Server media

Note: ISO is already mounted from previous steps. If not mounted then only execute below step.

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 directory path).

Note: Before starting the installation make sure all the three servers Admin, MS1, MS2 are in running state in weblogic console.

6.2.2 Install Management Server

As root, run:

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

During installation it will ask for below details

1. Admin server internal IP
2. MS1 server internal IP
3. MS2 server internal IP
4. Weblogic console user name
5. Weblogic console password
6. Database user password.

Please provide these values very carefully.

Wait until the installation process is complete.

Analyze the installation log:

Verify that Management server is installed successfully.

Review the Management server installation log (/var/log/nsp/install/nsp_install.log) for errors.

If It did not install successfully, contact the Oracle Support, 16. APPENDIX: My Oracle Support (MOS)

6.3 Management Server Post Installation Configuration

6.3.1 Restart Weblogic Servers

1. Log on to MS1 and MS2 servers respectively as root user and execute below command

```
# reboot
```

Wait for servers to come up

2. Log on to servers as root user and verify that node manager is running or not by executing below command.

```
# ps -eaf | grep java
```

Sample output of the command would look like this:

```
oracle 2844 2781 0 Mar18 ? 00:04:48 /opt/oracle/jdk1.6.0_45/bin/java -
client -Xms32m -Xmx200m -XX:MaxPermSize=128m -
```

```
Dcoherence.home=/opt/oracle/middleware/coherence_3.7 -
Dbea.home=/opt/oracle/middleware -Dverbose=true -DStartScriptEnabled=false -
DCrashRecoveryEnabled=true -DDomainRegistrationEnabled=true -DListenPort=5556 -
Xverify:none -
Djava.security.policy=/opt/oracle/middleware/wlserver_10.3/server/lib/weblogic.poli
cy -Dweblogic.nodemanager.javaHome=/opt/oracle/jdk1.6.0_45 weblogic.NodeManager -
v
```

In case if Node manager service is not running then do not proceed ahead and contact Oracle 16. APPENDIX: My Oracle Support (MOS)

3. Log on to AdminServer as root user and execute below command to restart Admin server

```
# reboot
Wait for some time after the AdminServer is up and then log on to weblogic console to verify the
servers state there. They must be "Running" and their health should be "ok". Post that verify wether
the jmx process is running on the system or not. Execute below command after log on to Admin
Server as root user
```

```
# ps -eaf | grep jmx
Sample output of the command would look like this:
```

```
[root@WL_ tekelec_AS ~]# ps -eaf | grep jmx
root      2882      1  0 04:49 ?          00:00:05 /opt/TKLCjmxagent/bin/wrapper
/opt/TKLCjmxagent/in/wrapper.conf wrapper.syslog.ident=JMXAgent
wrapper.pidfile=/opt/TKLCjmxagent/JMXAgent.pid wrapper.name=JMXAgent
wrapper.displayName=Tekelec JMX Agent wrapper.daemonize=TRUE
wrapper.lockfile=/var/lock/subsys/JMXAgent

root      2884  2882  0 04:49 ?          00:00:21
/opt/oracle/jdk1.6.0_45/jre/bin/java -Dcom.steleus.jmx.home=.. -
Dcom.steleus.jmx.log=/var/TKLC/log/jmxagent -Dweblogic.corba.client.bidir=true -
Xms256m -Xmx256m -Djava.library.path=../bin -classpath
../jar/com.steleus.jmx.jar:../jar/wrapper/wrapper.jar -
Dwrapper.key=mTPDAPowAawt1JECVW8Oh2YdOHqZmdOJ -Dwrapper.port=32000 -
Dwrapper.jvm.port.min=31000 -Dwrapper.jvm.port.max=31999 -
Dwrapper.disable_console_input=TRUE -Dwrapper.pid=2882 -Dwrapper.version=3.5.17-st
-Dwrapper.native_library=wrapper -Dwrapper.arch=x86 -Dwrapper.service=TRUE -
Dwrapper.cpu.timeout=10 -Dwrapper.jvmid=1 -Dwrapper.lang.domain=wrapper
com.steleus.jmx.Main
```

In case if servers state are not as mentioned above or jmxagent process is not running then do not proceed ahead and contact Oracle 16. APPENDIX: My Oracle Support (MOS)

6.3.2 Configure firewall and permissions on Admin server and copy required files to respective server.

1. Log on to Admin server as root user and execute below commands

```
# sh /opt/nsp/nsp-
package/framework/install/dist/install/post_installation/configureFirewall.sh
Expected output of the command is mentioned below:
net.ipv4.ip_forward = 1
Saving firewall rules to /etc/sysconfig/iptables:          [ OK ]
Flushing firewall rules:                                  [ OK ]
Setting chains to policy ACCEPT: nat filter                [ OK ]
Unloading iptables modules:                               [ OK ]
Applying iptables firewall rules:                         [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]

Execute below command to verify if the rules have been set
# iptables -L -n -t nat -v
Sample output in case of correct port forwarding rules:
[root@WL_ tekelec_AS ~]# iptables -L -n -t nat -v
```

PIC 10.1.5 Installation Guide

```
Chain PREROUTING (policy ACCEPT 57376 packets, 2381K bytes)
 pkts bytes target      prot opt in     out     source      destination
  363 21780 DNAT        tcp  --  eth1    *       0.0.0.0/0    10.31.2.82
tcp dpt:7001 to:192.168.16.64:7001

# chmod 700 /opt/nsp/.ssh
# chmod 600 /opt/nsp/.ssh/*
# su - tekelec -c "
scp /opt/nsp/nsp-
package/framework/install/dist/install/post_installation/configureFirewall.sh
oracle@<MS1_IP>:/home/oracle;
scp /opt/nsp/nsp-
package/framework/install/dist/install/post_installation/configureFirewall.sh
oracle@<MS2_IP>:/home/oracle;
scp /opt/nsp/nsp-
package/framework/install/dist/install/scripts/config_backup_user.sh
oracle@<ORACLE_IP>:/home/oracle;
scp /opt/nsp/nsp-package/framework/db/dist/utils/cmd/nsp_backup_job.sh oracle@<
ORACLE_IP>:/home/oracle
"
```

Replace <MS1_IP>, <MS2_IP> and <ORACLE_IP> with actual IPs.

6.3.3 Change the open file limit and configure firewall on MS1 and MS2 servers

1. Log on to MS1 server as root user and execute below command

```
# grep "NSP" /etc/security/limits.conf && echo "/etc/security/limits.conf already
updated." || cat >> /etc/security/limits.conf << _EOF_
# following lines added for NSP
* soft nofile 2048
* hard nofile 65536
_EOF_
#sh /home/oracle/configureFirewall.sh
```

Expected output of the command is mentioned below:

```
net.ipv4.ip_forward = 1
Saving firewall rules to /etc/sysconfig/iptables:          [ OK ]
Flushing firewall rules:                                  [ OK ]
Setting chains to policy ACCEPT: nat filter                [ OK ]
Unloading iptables modules:                               [ OK ]
Applying iptables firewall rules:                         [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]
```

Execute below command to verify if the rules have been set

```
# iptables -L -n -t nat -v
```

Sample output in case of correct port forwarding rules:

```
[root@WL_tekelec_MS1 ~]# iptables -L -n -t nat -v
Chain PREROUTING (policy ACCEPT 66755 packets, 2934K bytes)
 pkts bytes target      prot opt in     out     source      destination
  117  7020 DNAT        tcp  --  eth1    *       0.0.0.0/0    10.31.2.83
tcp dpt:7001 to:192.168.16.68:7001
```

2. Repeat step 1 for MS2 server also

6.3.4 Create directory structure and key sharing on Oracle server

1. Log on to oracle server as root user and execute below commands:

```
# mkdir -p /opt/nsp /opt/oracle/backup
# chown oracle:oinstall /opt/nsp /opt/oracle/backup
# ssh tekelec@<Admin server IP> "cat >> /opt/nsp/.ssh/authorized_keys " <
/home/oracle/.ssh/authorized_keys
```

Replace <Admin server IP> with actual IP. Respond with yes when it prompts.

6.3.5 Configure NFS server

1. Log on to NFS server and execute below commands to configure NFS.

```
# mkdir -p <DIR_PATH>
# chmod 777 <DIR_PATH>
# echo "<DIR_PATH> <ORACLE_IP>(rw,async,no_root_squash,nohide,anonuid=-1)" >>
/etc/exports
# service iptables stop
(In case it is already stopped above command will do nothing)
# service nfs restart
```

Here, DIR_PATH could be any directory path, ORACLE_IP is oracle server external IP

2. Log on to Oracle server and execute below commands to configure NFS.

```
# echo "<NFS_SERVER_IP>:<DIR_PATH> /opt/oracle/backup nfs
rw,bg,hard,rsize=32768,wsiz=32768,vers=3,nointr,timeo=600,tcp 0 0" >> /etc/fstab
# mount -a -t nfs
```

Here, DIR_PATH is the same path which is provided in step 1.

6.3.6 Schedule Management database backup job on oracle server

Log on to oracle server as root user and execute below commands to copy required files and to create backup user and schedule the management server backup job. It will execute PIC global backup first time as well.

```
# sh /home/oracle/nsp_backup_job.sh
The command output may report error,because the script first drops the job and re-
create it. During first time execution the job will not be present. Following
error can be ignored:
```

```
ERROR at line 1:
ORA-27475: "NSP.NSP_BACKUP_JOB" must be a job
ORA-06512: at "SYS.DBMS_ISCHED", line 224
ORA-06512: at "SYS.DBMS_SCHEDULER", line 657
ORA-06512: at line 2
```

The script should end in two following lines:
PL/SQL procedure successfully completed.
PL/SQL procedure successfully completed.

```
# sh /home/oracle/config_backup_user.sh
# scp -p /usr/lib64/libpcap.so.0.9.4 root@<Admin server IP>:/usr/lib64/
# scp -p /usr/lib64/libpcap.so.0.9.4 root@<MS1_IP>:/usr/lib64/
# scp -p /usr/lib64/libpcap.so.0.9.4 root@<MS2_IP>:/usr/lib64/
```

Respond with yes when it prompts.

6.3.7 Change Customer Icon (Optional)

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

1. Open a terminal window and log in as oracle on both Management servers MS1 and MS2.
2. Copy the customer icon file (customer_icon.jpg) to the /opt/www/nsp/resources directory of each server.
3. Verify the customer icon properties:

The file name must be customer_icon.jpg.

The file must belong to user oracle in group oinstall.

The compression format must be Jpeg.

Optimum width/height ratio is 1.25.

Any image can be used; the suggested minimum width/height is 150 pixels.

6.3.8 Install Optional Applications

This procedure describes how to install optional applications.

6.3.8.1 Applications list

- L99465 PIC Mediation DataFeed
- L99467 PIC Multiprotocol Troubleshooting Application
- L99468 PIC Network and Service Alarm Applications
- L99469 PIC Network and Service Dashboard
- L99470 PIC SS7 Network Surveillance Applications
- L99471 On Demand User Plane Capture Application
- Session Point Code

6.3.8.2 Applications installation

1. Open a terminal window and log in as tekelec on the Management Admin server.
2. Change dir to `/opt/nsp/nsp-package/framework/install/dist/install/optional/exec` folder
3. Change the permission of the executables by executing the below command:

```
# chmod a+x *
```

Below should be the updated permission:

```
-rwxr-xr-x 1 tekelec tekelec 13456 Jul  4 15:44  
L99465_PIC_Mediation_DataFeed.sh
```

4. Install the required optional application by running the corresponding executable for that application.

For example : To install optional application “PIC Network and Service Dashboard.sh” type the name of executable “L99469_PIC_Network_and_Service_Dashboard.sh” and hit enter command

5. The install logs are available at `/var/log/nsp/install/activate_optional.log`.

6.3.9 Configure Purchased Tokens

This procedure describes how to increase purchased token after NSP is installed

1. Open a terminal window and log in as tekelec on the Management server.
2. Change dir to `/opt/nsp/nsp-package/framework/install/dist/install/optional/exec` folder
3. Change the permission of the executables by executing the below command:

```
# chmod a+x L99466_PIC_Management_Application.sh
```

Below should be the updated permission:

```
-rwxr-xr-x 1 tekelec tekelec 13720 Jul  4 15:44  
L99466_PIC_Management_Application.sh
```

4. Run the `L99466_PIC_Management_Application.sh` executable provided. It will prompt for number of concurrent user (The number of user sold for). Enter the value.
Note: User can not decrease the number of tokens. Value can be increased only. Maximum value can be 50 only.
5. After the value provided it will successfully increase the token.

6.3.10 Configure Open file limit for OTD (Mandatory)

1. Login to OTD Admin Node(s) (managed server) as root.
2. Execute

```
# cd /u01/OTDInstanceHome/net-wlsoda-otd-config1/bin/
```

3. open startserv script using vi editor
add a line "ulimit -n 131072" just before the enable_failover() is defined.
4. Stop the server instance by executing

```
./stopserv
```

5. Start the server instance by executing

```
./startserv
```

Note: Please see MOS documents [Doc ID 1610613.1](#) and [Doc ID 1564602.1](#) and SR [SR 3-10624968651](#) for further details.

6.3.11 Configure Weblogic Plug-In (Mandatory)

This procedure is required to enable the https access thorough OTD for the management server GUI. The procedure must be executed on each of the managed server using the weblogic admin console.

1. Log on to Weblogic console and click on Lock & Edit button.
2. In the Environment tab, click 'Servers'
3. Click on Managed Server(s) e.g. ms1 - in the Configuration, General - go to Advanced section.
4. Check the checkbox with the text 'WebLogic Plug-In Enabled'.
5. Save and Activate the changes.
6. Restart the managed servers from the weblogic console.

Note: For other optional procedures on management server refer [PIC 10.1.5 Maintenance Guide, E56062, Chapter 7](#)

6.4 Management Server Post Install Health Check

Box: Admin Server

1. Open a terminal window and log in as root on the Admin Server.
2. Review the Management Server installation logs (/var/log/nsp/install/nsp_install.log).
- 3) Log on to weblogic console and Verify the following:
 - All servers are in running and in OK state
 - Oracle em console connectivity is OK
 - Application deployments are in Active and OK state.

7 ACQUISITION SERVER APPLICATION INSTALLATION PROCEDURES

This section provides the procedures for installing the acquisition server application.

Note: This step should be executed for all the servers in sub-system.

7.1 Pre-Install Configuration

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

7.1.1 Temporary customer IP assignment

This procedure provides instructions to temporary customer IP assignment to transfer the Application ISO on server during installation.

Note: This procedure is only to be used to transfer the Application ISO during installation.

Configure Vlan tagging and assign ip address in case of Integrated Acquisition Server

- a) Login via ILO, iLOM, to server as root
- b) Execute following commands (1st line for E5-APP-B only):

```
# ifconfig eth01 up
# modprobe 8021q
# vconfig add eth01 200
# ifconfig eth01.200 <CUST IP ADDRESS> netmask <MASK>
# route add default gw <DEFAULT ROUTE IP ADDRESS>
```

Assign ip address in case of Probed Acquisition Server: see [APPENDIX: Manual configuration of ethernet interfaces](#)

7.1.2 Copy ISO

- a) Transfer acquisition server ISO on the server to /var/TKLC/upgrade directory
- b) Verify that ISO file is transferred completely on the server.

7.1.3 Configure server

This procedure describes how to configure the acquisition servers prior to installing the application.

Note: This procedure must be executed on all of the Integrated and Probed acquisition servers.

1. Change the current hostname, designation and function

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

- a) Enter the platcfg menu, as root run:
su - platcfg
- b) Select Server Configuration->Hostname
- c) Select Edit
- d) Set the hostname
- e) Select Server Configuration -> Designation/Function.
- f) Select Edit.
- g) Change the designation and function.

- For a Integrated Acquisition subsystem:
In the Designation field, enter the designation in the following format: 1A for the first server, 1B for the second, and so on. In the Function field, enter IMF.
- For a standalone Probed Acquisition:
In the Designation field, enter the 0A for the server. In the Function field, enter PMF.

h) Select Exit.

2. Install the bulkconfig file

Note: Before you perform this procedure, make sure you have read and are familiar with the [11.4 Acquisition Server Bulkconfig File Description](#)

7.2 Acquisition Server Pre-Install Healthcheck

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

Log in as root on the server that you want to install the acquisition server application.

Run:

```
# syscheck
```

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

Example output for a healthy system:

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

Running modules in class hardware...
                OK

Running modules in class net...
                OK

Running modules in class proc...
                OK

Running modules in class system...
                OK

Running modules in class upgrade...
                OK
```

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

7.3 Install Acquisition Server Application

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

Note: Run this procedure from iLO console

1. Log in as root user
2. Enter the platcfg menu, as root run:

PIC 10.1.5 Installation Guide

```
# su – platcfg
```

3. Select Maintenance ► Upgrade ► Initiate Upgrade.
4. Select the acquisition server application media and press Enter.

Informational messages appear on the terminal screen as the upgrade proceeds. When installation is complete, the server reboots and displays the login prompt.

You can check the TPD upgrade log file (/var/TKLC/log/upgrade/upgrade.log) for any error; but the status of the server will be checked when you run the healthcheck script after you configure the switches.

7.4 Configure Site and Subsystem for Acquisition Server

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

The subsystem is treated by PIC as a cluster, accessible by Management Server through this IP address.

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

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

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

1. Log in to the Management server application

- a) Log in as tekelec to the Management server application interface using the management server one box's IP address or OTD server's VIP address.
- b) Click **Centralized configuration**.

2. Create a site on CCM

- a) Select **Equipment Registry ► Sites ► Add**.
- b) Type the desired site name and click **Add**.

3. Create Acquisition sub-system and Add the server(s) on Management Server

Note: Skip this step if the Site already exists.

- a) Select **Equipment Registry ► Sites ► *New site name created* ► XMF ► Add**
- b) Type the server IP address(es) for the xMF subsystem and click **Add**.
- c) Click **Create**.

7.5 Acquisition Server Healthcheck post customer integration

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

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

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

```
$ analyze_subsystem.sh
```

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

If the error occurs, contact Oracle Support using [16. APPENDIX: My Oracle Support \(MOS\)](#)

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

Example output for a healthy subsystem:

```
-----
ANALYSIS OF SERVER IMF0907-1A STARTED
-----

FIPS integrity verification test failed.
08:24:59: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
08:24:59: date: 05-17-15, hostname: IMF0907-1A
08:25:00: TPD VERSION: 7.0.1.0.0-86.20.0
FIPS integrity verification test failed.
08:25:00: XMF VERSION: [ 10.1.5.0.0-3.3.0 ]
FIPS integrity verification test failed.
08:25:00: -----
08:25:01: Checking disk free space
08:25:01:   No disk space issues found
08:25:01: Checking syscheck - this can take a while
08:25:18:   No errors in syscheck modules
08:25:18: Checking statefiles
08:25:19:   Statefiles do not exist
08:25:19: Checking runlevel
08:25:19:   Runlevel is OK (4)
08:25:20: Checking upgrade log
08:25:20:   Install logs are free of errors
08:25:21: Analyzing date
08:25:21:   NTP daemon is running
08:25:21:   IP of NTP server is set
08:25:22:   Server is synchronized with ntp server
08:25:22: Analyzing IDB state
08:25:23:   IDB in START state
08:25:23: Checking IDB database
08:25:24:   iaudit has not found any errors
08:25:24: Analyzing processes
08:25:25:   Processes analysis done
08:25:26: Analysing database synchronization
08:25:26:   Either Database synchronization in healthy state or errors found are non-blocking
08:25:27: Checking weblogic server entry
```

PIC 10.1.5 Installation Guide

```
08:25:27: Appserver is present
08:25:27: Checking whether ssh dsa key was generated
08:25:28: dsa key is generated
08:25:28: Checking whether ssh keys are exchanged among machines in frame - this can take a
while
08:25:29: 1 mates found: yellow-1B
08:25:35: Connection to all mates without password was successful
08:25:35: All tests passed. Good job!
08:25:36: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0907-1A

-----
ANALYSIS OF SERVER IMF0907-1B STARTED
-----

VPATH=/tekelec/TKLCmf/runtime:/opt/TKLCmf
PRODPATH=/opt/TKLCcomcol/cm6.4
RUNID=00
PRODID=
08:25:01: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
08:25:02: date: 05-17-15, hostname: IMF0907-1B
08:25:02: TPD VERSION: 7.0.1.0.0-86.20.0
08:25:02: XMF VERSION: [ 10.1.5.0.0-3.3.0 ]
08:25:03: -----
08:25:03: Checking disk free space
08:25:03: No disk space issues found
08:25:04: Checking syscheck - this can take a while
08:25:13: No errors in syscheck modules
08:25:14: Checking statefiles
08:25:14: Statefiles do not exist
08:25:14: Checking runlevel
08:25:15: Runlevel is OK (4)
08:25:15: Checking upgrade log
08:25:16: Install logs are free of errors
08:25:16: Analyzing date
08:25:16: NTP daemon is running
08:25:17: IP of NTP server is set
08:25:17: Server is synchronized with ntp server
08:25:17: Analyzing IDB state
08:25:18: IDB in START state
08:25:18: Checking IDB database
08:25:19: iaudit has not found any errors
08:25:19: Analyzing processes
08:25:20: Processes analysis done
08:25:20: Analysing database synchronization
08:25:21: Either Database synchronization in healthy state or errors found are non-blocking
08:25:21: Checking weblogic server entry
08:25:22: Appserver is present
08:25:22: Checking whether ssh dsa key was generated
08:25:22: dsa key is generated
08:25:23: Checking whether ssh keys are exchanged among machines in frame - this can take a
while
```

```
08:25:23: 1 mates found: yellow-1A
08:25:30: Connection to all mates without password was successful
08:25:30: All tests passed. Good job!
08:25:30: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0907-1B
```

```
IMF0907-1A TPD: 7.0.1.0.0-86.20.0 XMF: 10.1.5.0.0-3.3.0 0 test(s) failed
IMF0907-1B TPD: 7.0.1.0.0-86.20.0 XMF: 10.1.5.0.0-3.3.0 0 test(s) failed
```

Example output for a subsystem with errors:

```
END OF ANALYSIS OF SERVER IMF0502-1D
IMF0502-1A TPD: 7.0.1.0.0-86.20.0 XMF: 10.1.5.0.0-3.3.0 1 test(s) failed
IMF0502-1B TPD: 7.0.1.0.0-86.20.0 XMF: 10.1.5.0.0-3.3.0 3 test(s) failed
server on interface yellow-1c is not accessible (ping)
IMF0502-1D TPD: 7.0.1.0.0-86.20.0 XMF: 10.1.5.0.0-3.3.0 0 test(s) failed
Differences between tpd platform versions found!
Differences between message feeder application versions found!
```

8 DATA RECORD STORAGE INSTALLATION PROCEDURES

8.1 Configure Data Record Storage on ODA

Note : This section must be executed for ODA based DRS server only.

To create schema, install DTO package and to schedule jobs there is a consolidated script “installExtDWS.sh”.

Execute following command(s) (from oracle user with ORACLE_HOME and ORACLE_SID set as mentioned in section 4.4):

```
# cd /mnt/upgrade/migration/oracle/instance/cmd/
# ./installExtDWS.sh IXP/*** <SYS_CONNECTION_STRING>
```

Where, <SYS_CONNECTION_STRING> is in format SYS/<SYS_password> and <SYS_password> is system password, which should be “*****”.

Note: In logs there will be many spool log error which should be ignored. Verify the logs for errors other than spool log error.

The DR storage database creation is complete and it can be discovered on management server.

8.2 Configure Oracle on ODA based Data Record Storage

This step can be performed after the discovery of DR Storage on management server.

Note: Mount the ISO using root user if the ISO is not already mounted.

To create data and index file(s) on ODA based DR Storage there is a separate script, which can be executed from ODA database server or from remote mediation base server.

It is suggested to create the data and index files in the ratio of 30 and 20 (data: index is 30:20), of the space allocated from the total available space.

1. Obtain total available space.

ODA database server: The total space and available space can be found by following commands :

```
# su - oracle
# export ORACLE_SID=IXP
# ORAENV_ASK=NO source oraenv
# cd /mnt/upgrade/migration/oracle/utils/cmd/
# ./CreateDataAndIndexFile.sh -c IXP/IXP
```

Or

Remote Mediation Server: The total space and available space can be found by following commands:

```
# su - cfguser
# cd oracle_utils
# ./CreateDataAndIndexFile.sh -c IXP/IXP@<IPAddressOfDWS>/IXP
```

2. Obtain number of data and index files that can be created within provided percentage usage from command line.

ODA database server: The number of data and index files that can be created within provided percentage of space can be found by following commands :

```
# ./CreateDataAndIndexFile.sh -c IXP/IXP -p <PERCENT_USE>
```

Or

Remote Mediation Server: The number of data and index files that can be created within provided percentage of space can be found by following commands:

```
# ./CreateDataAndIndexFile.sh -c IXP/IXP@<IPAddressOfDWS>/IXP -p
<PERCENT_USE>
```

3. Create data and index files.

In the following command if the percentage switch <PERCENT_USE> is not provided then it creates the data and index files in ratio of 30 and 20 (data: index is 30:20), reserving 10% of total space from available space, else it will use <PERCENT_USE> percent of available space to create data and index file.

ODA database server:

```
# ./CreateDataAndIndexFile.sh -c IXP/IXP -p <PERCENT_USE> -r
```

Or

Remote Mediation Server:

```
# ./CreateDataAndIndexFile.sh -c IXP/IXP@<IPAddressOfDWS>/IXP -p
<PERCENT_USE> -r
```

Where, <PERCENT_USE> is an integer value greater than 0 and less than 100. It is the percentage of available usable space user want to allocate for data and index file creation.

This procedure can take a very long time (up to 5 hours).

4. Unmount the mediation server ISO from ODA database server as root user:

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

8.3 Add Data Record Storage to CCM

This procedure describes how to add the DWS to the CCM on Management Server. This procedure is performed through the Management application interface.

1. Log in to the Management server GUI and open Centralized Configuration (CCM)
 - a) Log in to the NSP application interface as tekelec using the Management server IP address.
 - b) Open the Centralized Configuration application.
 - c) Select Equipment Registry.
2. Configure the new site
 - a) Right-click the Sites list and select Add to enter new site configuration.
 - b) Type the Site name and Description and click Add.
3. Add the DWS to the site
 - a) Navigate to Sites.
 - b) Right-click DWH and select Add to enter the DWS configuration:
 - o Fill the DWS server hostname into the Storage Name field.
 - o Fill the Login user Id (IXP by default)
 - o Fill the Password (Refer to TR006061 for the default value)

PIC 10.1.5 Installation Guide

- Fill the Service Name (IXP by default)
- Fill in the IP address of the DWS.

Note: If the DWS added is the same storage pool then it must have the same capacity in terms of storage. The number of DATA_CDR and DATA_IND files should be same and of same size.

- c) Click Add.

9 MEDIATION APPLICATION INSTALLATION PROCEDURES

This section provides the procedures for installing the Integrated xDR Platform (MEDIATION) application.

Warning: The procedures must only be executed on Meduaction Base servers and must not be executed on Mediation PDU servers.

9.1 Mediation Server Pre-Install Configuration

This procedure describes how to configure mediation server prior to installing the application.

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

Note: When creating a bulkconfig file on a server in the Mediation subsystem, if such a file has already been created on a different server, then reuse that bulkconfig file. The content of the bulkconfig file is the same for all servers in the Mediation subsystem.

9.1.1 Verify each server healthcheck.

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

```
# syscheck
```

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

Example output of healthy server:

```
Example ouput for a healthy system:
```

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

```
OK
```

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

```
OK
```

```
Running modules in class net...
```

```
OK
```

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

```
OK
```

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

```
OK
```

```
Running modules in class upgrade...
```

```
OK
```

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

Resolve each error before you continue with the procedure.

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

Note: Step b and c has to be executed if error occur in this step.

PIC 10.1.5 Installation Guide

9.1.2 Configure Bonding Interface (Optional)

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) Login into the mediation server's console
- 2) To create the bonding interface, 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
```

- 3) To create the default route, as root, run:

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

9.1.3 Create the bulkconfig file

1. As a root user.
2. Create the /root/bulkconfig file as explained in annex MEDIATION Bulkconfig File Description.

Note: Be sure to have one `host` entry per MEDIATION server in the bulkconfig file. Enter the hostname as `ixpNNNN-MA`, with:

- o the same **NNNN** designation (4 digits) for all the servers of the MEDIATION subsystem and the same as for the related DWS
- o the same **M** designation (1 digit, excluding "0") for all the servers for the MEDIATION subsystem and the same as for the related DWS
- o as its **A** designation (a small letter), "a" for the first server in this MEDIATION subsystem, "b" for the second server, and so on...

Note: In the `bulkconfig` file, be sure to use the `bond0` interface (and not the usual `ethxx` interface)

9.1.4 Configure the server hostname

1. Enter the `platcfg` menu.

As root, run:

```
# su - platcfg
```

2. Select **Server Configuration -> Hostname**
3. Click **Edit**.
4. Enter the server hostname in the standard format: `ixpNNNN-MA` (see section 9.1.3 for naming details).
5. Exit the `platcfg` menu.

9.2 Install Mediation Server

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

Before you perform this procedure, make sure that you have the appropriate mediation server ISO file available.

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

Note: Run this procedure via iLO.

9.2.1 Temporary customer IP assignment

This procedure provides instructions to temporary customer IP assignment to transfer the Application ISO on server during installation.

Note: This procedure is only to be used to transfer the Application ISO during installation.

Refer to [APPENDIX: Manual configuration of ethernet interfaces](#)

Note: The temporary customer IP assignment is not to be executed if a bonding interface has been setup

9.2.2 Copy ISO

1. Copy mediation server iso to /var/TKLC/upgrade folder.

9.2.3 Install the application

1. From platcfg menu select Maintenance -> Upgrade -> Initiate Upgrade.

When the installation process is complete, the server restarts automatically.

Note: after the server has restarted, at login, a message asking to accept or reject the upgrade is displayed: the message can be safely ignored until the Integrate Customer Network step has been executed.

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

As root, run:

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

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

9.2.4 Analyze the installation log

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

If there are any errors, contact the Oracle Support Team at [APPENDIX: My Oracle Support \(MOS\)](#)

9.3 Mediation Server Post-Install Healthcheck

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

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

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

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

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

PIC 10.1.5 Installation Guide

Example of overall output:

```
08:43:58: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
08:43:59: date: 05-17-15, hostname: ixp0907-1a
08:43:59: TPD VERSION: 7.0.1.0.0-86.20.0
08:44:00: IXP VERSION: [ 10.1.5.0.0-3.2.0 ]
08:44:00: XDR BUILDERS VERSION: package TKLCxdrbuilders is not
installed
08:44:00: -----
08:44:01: Analyzing server record in /etc/hosts
08:44:01:     Server ixp0907-1a properly reflected in /etc/hosts file
08:44:02: Analyzing IDB state
08:44:02:     IDB in START state
08:44:03: Analyzing shared memory settings
08:44:03:     Shared memory set properly
08:44:04: Analyzing IXP Licence
08:44:05:     Ixp Licence Valid
08:44:05: Analyzing mount permissions
08:44:05:     Writing enabled for pdu_1
08:44:06:     Writing enabled for pdu_2
08:44:06:     All mount permissions set properly
08:44:06: Analyzing date
08:44:07:     NTP deamon is running
08:44:07:     IP of NTP server is set
08:44:08: Checking CPU usage
08:44:08:     CPU usage check done
08:44:08: Running iaudit
08:44:10:     iaudit did not find any errors
08:44:10: Analyzing disk usage
08:44:11:     Space not exceeded
08:44:11: Analyzing JMX agent properties
08:44:12:     Instance ID of JMX agent OK
08:44:13:     IxpMbean [ application type IXP+2 ] located
08:44:13: Checking syscheck - this can take a while
08:44:17:     No active alarms
08:44:17: Checking services
08:44:17:     NFS service is running
08:44:18:     Portmap service is running
08:44:18: Analyzing bulkconfig content
08:44:19:     BulkConfig content is consistent
08:44:19: All tests passed!
08:44:19: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
```

Example of a failed test:

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

Note: if the following error shows up during server analysis, it can be simply ignored, as the alarm will be cleared after Integrate Customer Network step (see below) will have been executed.

```
12:21:48: >>> Error: Alarm raised for tpdServerUpgradePendingAccept...
12:21:48: >>> Suggestion: Check /var/TKLC/log/syscheck/fail_log...
```

In any other cases, after attempting the suggested resolution, if the test fails again, then contact 16. APPENDIX: My Oracle Support (MOS)

9.4 Integrate Customer Network

This procedure describes how to integrate the mediation subsystem post-manufacturing customer network.

This procedure uses the `/root/bulkconfig` file as an input for the customer network integration. Before you perform this procedure, make sure you have read and are familiar with the [11.2 Mediation Server Bulkconfig File Description](#).

This procedure is run from the iLO.

1. Update the bulkconfig file
 - a) Log in on the iLO of **any Mediation server** in the Mediation subsystem that you want to reconfigure.
 - b) Update the `/root/bulkconfig` file with the customer IP addresses and timezone.
 - c) Make entries for PDU mounts for external PDU storage in bulkconfig file.

Note: The step c) shall take care of the case where the PDU storage is done on ZFS server. The customer integration step shall automatically take into account the shared NFS mount points created on ZFS.

2. Run the customer network integration
 - a) Run the mediation subsystem customer network integration script. As root, run:


```
# bc_customer_integration.sh
```
 - b) Confirm this operation.
Enter yes.
A prompt for the root password appears.
 - c) Provide the root password.
The servers reboot.

3. Run the post-integration settings

Note: The mediation server has new IP address. The previous addresses are no longer accessible.

- a) Run post-integration settings. As root, run:


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

A prompt for the root and cfguser passwords appears.

Note: The key exchange operation is part of this script.

- b) Provide the appropriate passwords.
When the script is complete, check the terminal output for any errors. If the error occurs, contact the 16. APPENDIX: My Oracle Support (MOS)

9.5 Add Mediation Subsystem to CCM

This procedure describes how to add the Mediation subsystem to the CCM on Management server. This procedure is performed through the NSP application interface.

For an estimated time for this procedure, refer to the mediation subsystem overview flowchart.

Note: a pool of DWS (it can be one single DWS) must already have been declared in CCM. A pool of DWS cannot be the primary xDR storage of several mediation subsystems (the primary xDR storage is the DWS pool that is selected when the mediation subsystem is declared in CCM).

1. Log in to the NSP and open Centralized Configuration (CCM)
 - a) Log in to the NSP application interface as tekelec using the Management Server Apache/Onebox server IP address.
 - b) Open the Centralized Configuration application.
 - c) Select Equipment Registry.
2. Configure the new site

Note: Configure new site only if earlier created site does not exist.

 - a) Right-click the Sites list and select Add to enter new site configuration.
 - b) Type the Site name and Description and click Add.
3. Add the mediation subsystem to the site
 - a) Navigate to Sites.
 - b) Right-click IXP and select Add to enter the mediation subsystem configuration.
 - c) Type values for the following fields:
 - Mediation subsystem name in **Subsystem Name**
 - Dedicated IP address for the mediation subsystem in **VIP Address**.

Note: The Virtual IP (VIP) Address is an actual IP address in the same subsystem subnet that is not physically used by any other server or equipment. The subsystem is treated by Management Server as a cluster accessible from Management Server through this IP address.
 - IP address of the mediation server
 - d) Click Add.
 - e) Repeat steps 3.b.-3.d for each server in the mediation subsystem.
 - f) Verify that all of the added servers are listed in the Locations list.
 - g) Select the DWS pool to use as primary xDR storage.
 - h) Click Create.

Information is synchronized from the mediation servers to the Management Server.
4. Apply the configuration changes
 - a) Navigate to **Mediation** tab.
 - b) In the left-hand menu, open **Sites**, open the site on which the Mediation subsystem has been created, open IXP and right-click the Mediation subsystem name.
 - c) Select **Apply changes...** and click **Next, Next, Apply changes**
 - d) Confirm by clicking **OK**
 - e) Click **Done** when the changes have been applied

Note: "Unable to update or create capacity management session" warning must be ignored during Apply Change.

9.6 Install xDR Builders

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

1. Log in on the Management Server Admin server and insert the xDR DVD/CD or copy the ISO file at /var/TKLC/upgrade, if it exists. If not then create it.

Note: Don't copy the builder ISO at root directory.

- a) Open a terminal window and log in on the Management Server Admin server.
- b) Insert the xDR Builders DVD/CD or copy the xDR Builder ISO file to the Management Server Admin server.

2. Run the install script

- a) As root, run:

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

The following prompt appears:

Please enter path to Builder ISO [/media/cdrom]:

- b) Enter the appropriate response based on the media used:
 - For a DVD/CD, press **Enter**.
 - For an ISO file, enter the exact path including the ISO file name.
- c) Wait until the installation is complete.

Note: the script will ask password for oracle user many times.

3. Verify the ISO installation on Management Server

- a) Open a web browser and log in as TklcSrv on the management server application interface.
- b) Open the **Upgrade Utility**.
- c) Click **Manage Builder Rpm** in the left tree.

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

4. Upload Builders RPM

- a) Select the desired xDR Builder RPM with the **Not Uploaded** state and click **Upload**. A confirmation window appears.
- b) Click **Continue** to continue the RPM upload.

If the upload is successful, then the RPM state changes to **Uploaded**. If the upload fail contact the Oracle Support, 16. APPENDIX: My Oracle Support (MOS)

5. Associate the xDR Builders RPM with the Mediation subsystem

- a) Click **View Builder RPM Status** in the left tree. A list of the Mediation subsystems appears.
- b) Select one or more Mediation subsystems and click **Associate RPM Package**. A list of Builder RPMs that are uploaded in Management Server appears.

PIC 10.1.5 Installation Guide

- c) Select the appropriate xDR Builder RPM and click **Associate**.
If the association is successful, then the list of the subsystems is updated. The **RPM Name** column contains the new RPM package name and **Association Status** is marked as **OK**. If the association fails contact the Oracle Support, 16. APPENDIX: My Oracle Support (MOS)
6. Apply the configuration to the Mediation subsystem
 - a) Return to the main page of the NSP application interface.
 - b) Open the **Centralized Configuration** application.
 - c) Navigate to **Mediation**.
 - d) Open **Sites** and open the site; then, open **IXP**.
 - a) Right-click the subsystem and select **Apply changes....**
 - b) Click **Next**.
 - c) Click **Apply Changes**.
 - d) When change is complete, verify there are no errors on the result page.
7. Install the xDR Builders RPM on Mediation Server
 - a) Return to the main page of the NSP application interface.
 - b) Open the **Upgrade Utility**.
 - c) Click **View Builder RPM Status** in the left tree.
The available MEDIATION subsystem with their respective RPM Associate Status and Install Status appears.
 - d) Before initiating the builder installation, make sure the **Builder RPM** that you want to install on the MEDIATION subsystem is associated with the MEDIATION subsystem as indicated by **RPM Name** column and **Association Status** marked as **OK**. Also, **Install Status** should contain either - or **No Started**.
 - e) Select one or more Mediation subsystems and click **Install RPM Package**. If the installation is successful, the **Install status** changes to **OK**. If the installation fails contact Oracle Support, 16. APPENDIX: My Oracle Support (MOS)

9.7 Capacity Management KPIs installation

Capacity Management is a statistical session is generated with a dedicated xDR builder.

It provides very detailed self-surveillance data which can be better analyzed after selection and aggregation.

Derived statistical data are produced in real time (periodicity at the minute, quarter of hour and hour).

These statistical results are stored as regular xDR, which allows to manage this with standard PIC tools (such as ProTrace or ProPerf).

They globally provide system activity information in real time and an historical, traffic volume and verify the accuracy according to licenses.

Standard KPI configurations are provided and need mandatory installation steps. In addition optional customized KPI configurations could be added for more perspectives.

9.7.1 Installation Procedures for Capacity Management standard KPIs

This procedure describes how to deploy all needed elements for PIC system monitoring. This procedure is essential for license controls and this deployment is NOT optional.

1. CapacityManagement statistical session deployment

- a) All elements such as dedicated streams and DataFlows for this statistical session are automatically created as part of system deployment.
Naming convention makes that needed elements will contain *CapacityManagement* in the name (generally as suffix).
- b) Each time a new equipment such as Mediation or Acquisition server will be added to the system, it will be taken into account by CCM to create all new needed *CapacityManagement* elements. This mechanism will be done by a check at each configuration changes.
- c) You must check whether these elements have been correctly deployed or not (by using CCM and verifying presence or not of dedicated streams and DFP).
If not, please contact Support team in order to have the needed elements deployed for further usage of *Capacity Management*.

2. ProTraq templates deployment

- a) A set of ProTraq templates is provided. 3 configurations must be deployed (no automatic feature for this operation):
 - **PIC_UsageStat_Mn**: applied on *CapacityManagement*, provides consolidation / conversion of input Mbps for probed acquisition (PMF), integrated acquisition (IMF) and mediation (MEDIATION) over 1 mn. To apply on the basic statistical session *CapacityManagement* which is part of the standard deployment. Refer to [APPENDIX: Capacity Management ProTraq configurations](#)
 - **PIC_UsageStat**: applied on *PIC_UsageStat_Mn* result stat session; Agregation of *PIC_UsageStat_Mn* results over 15 minutes. Provides average, minimum, maximum throughput. To apply on the *PIC_UsageStats_Mn* statistical session (generated from the ProTraq configuration template **PIC_UsageStat_Mn**). Refer to [APPENDIX: Capacity Management ProTraq configurations](#)
 - **PIC_ActivityStat**: applied on *CapacityManagement*; Aggregation of key output data flows over 15 minutes, per destination for acquisition server and per final XB for mediation server in Kbps and efficiency. To apply on the basic statistical session *CapacityManagement* which is part of the standard deployment. Refer to [Capacity management good practices](#) (Doc ID 1683859.2) on My Oracle Support

The ProTraq configurations will have to be saved as text files before being imported into ProTraq application, on Management Server. Refer to ProTraq user guide to learn how to import ProTraq configurations and apply them to sessions.

- b) Activate the configurations
- c) Check the results: the statistical sessions must be created and should contain results. After one minute for *PIC_UsageStats* and after end of next quarter for the 2 others.

For deeper usages of *Capacity Management* please refer to the dedicated document (e.g. MEDIATION and Acquisition Server troubleshooting guides).

9.8 Mediation Subsystem Healthcheck

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

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

```
$ analyze_subsystem.sh
```

PIC 10.1.5 Installation Guide

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

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

Example of overall output:

```
$ analyze_subsystem.sh
-----
ANALYSIS OF SERVER ixp0907-1a STARTED
-----
09:39:25: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
09:39:25: date: 05-17-15, hostname: ixp0907-1a
09:39:25: TPD VERSION: 7.0.1.0.0-86.20.0
09:39:26: IXP VERSION: [ 10.1.5.0.0-3.2.0 ]
09:39:26: XDR BUILDERS VERSION: package TKLCxdrbuilders is not installed
09:39:27: -----
09:39:27: Analyzing server record in /etc/hosts
09:39:28:     Server ixp0907-1a properly reflected in /etc/hosts file
09:39:28: Analyzing IDB state
09:39:29:     IDB in START state
09:39:29: Analyzing shared memory settings
09:39:30:     Shared memory set properly
09:39:30: Analyzing IXP Licence
09:39:31:     Ixp Licence Valid
09:39:31: Analyzing mount permissions
09:39:32:     Writing enabled for pdu_1
09:39:32:     Writing enabled for pdu_2
09:39:33:     All mount permissions set properly
09:39:33: Analyzing date
09:39:33:     NTP daemon is running
09:39:34:     IP of NTP server is set
09:39:34: Checking CPU usage
09:39:34:     CPU usage check done
09:39:35: Running iaudit
09:39:36:     iaudit did not find any errors
09:39:37: Analyzing synchronization of server
09:39:38:     Role of server is StbMaster
09:39:38:     ActMaster server - ixp0907-1b
09:39:39:     StbMaster server - ixp0907-1a
09:39:40:     Server synchronizing properly
09:39:40: Analyzing NSP servers settings
09:39:41:     nsp_primary reflected in /etc/hosts
09:39:41:     Ping to nsp_primary OK
09:39:42:     nsp_secondary reflected in /etc/hosts
09:39:42:     Ping to nsp_secondary OK
09:39:42:     nsp_oracle reflected in /etc/hosts
09:39:43:     Ping to nsp_oracle OK
09:39:43:     Oracle on nsp_oracle accessible
09:39:44: Analyzing disk usage
09:39:44:     Space not exceeded
09:39:45: Analyzing JMX agent properties
09:39:45:     Instance ID of JMX agent OK
09:39:47:     IxpMbean [ application type IXP+2 ] located
09:39:47: Checking syscheck - this can take a while
09:39:49:     No active alarms
09:39:50: Checking services
09:39:50:     NFS service is running
09:39:51:     Portmap service is running
09:39:51: Analyzing ssh keys
```

```

09:39:51:      Ping to ixp0907-1a OK
09:39:52:      Ping to ixp0907-1b OK
09:39:52:      Ping to ixp0907-1c OK
09:39:52:      Ping to ixp0907-1d OK
09:39:53:      All keys for cfguser accounts exchanged
09:39:53: Analyzing DaqServer table in IDB
09:39:54:      Server ixp0907-1a reflected in DaqServer table
09:39:55:      Server ixp0907-1b reflected in DaqServer table
09:39:55:      Server ixp0907-1c reflected in DaqServer table
09:39:56:      Server ixp0907-1d reflected in DaqServer table
09:39:58:      VIP is set in DaqSubSystem table
09:39:59:      VIP is set in HaVipDef table
09:39:59:      Ping to 10.250.70.115 OK
09:40:00:      VIP is accessible
09:40:00: Analyzing processes
09:40:29: >>> Error: There are too many Dataflow processings (18). Should be 10
at most
09:40:29: >>> Suggestion: Dataflows should be redistributed to other servers
09:40:30:      Processes analysis done
09:40:30: Analyzing Data Feed status
09:40:31:      Data Feed analysis OK
09:40:31:      pdu_1 found in /etc/exports
09:40:32:      pdu_2 found in /etc/exports
09:40:32: Analyzing bulkconfig content
09:40:33:      BulkConfig content is consistent
09:40:33: All tests passed!
09:40:33: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp0907-1a

```

```

-----
ANALYSIS OF SERVER ixp0907-1b STARTED
-----

```

```

09:40:38: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
09:40:39: date: 05-17-15, hostname: ixp0907-1b
09:40:39: TPD VERSION: 7.0.1.0.0-86.20.0
09:40:39: IXP VERSION: [ 10.1.5.0.0-3.2.0 ]
09:40:40: XDR BUILDERS VERSION: [ 10.1.5.0.0-3.2.0 ]
09:40:40: -----
09:40:41: Analyzing server record in /etc/hosts
09:40:41:      Server ixp0907-1b properly reflected in /etc/hosts file
09:40:41: Analyzing IDB state
09:40:42:      IDB in START state
09:40:43: Analyzing shared memory settings
09:40:43:      Shared memory set properly
09:40:44: Analyzing IXP Licence
09:40:44:      Ixp Licence Valid
09:40:45: Analyzing mount permissions
09:40:45:      Writing enabled for pdu_1
09:40:45:      Writing enabled for pdu_2
09:40:46:      All mount permissions set properly
09:40:46: Analyzing date
09:40:47:      NTP deamon is running
09:40:47:      IP of NTP server is set
09:40:47: Checking CPU usage
09:40:48: >>> Warning: Process IxpBuild -id 43347 [ pid: 6637 ] is taking 96.3%
of CPU
09:40:48:      CPU usage check done
09:40:49: Running iaudit
09:40:50:      iaudit did not find any errors
09:40:51: Analyzing synchronization of server
09:40:52:      Role of server is ActMaster
09:40:52:      ActMaster server - ixp0907-1b
09:40:53:      StbMaster server - ixp0907-1a

```

PIC 10.1.5 Installation Guide

```
09:40:55:      Server synchronizing properly
09:40:56: Analyzing NSP servers settings
09:40:56:      nsp_primary reflected in /etc/hosts
09:40:56:      Ping to nsp_primary OK
09:40:57:      nsp_secondary reflected in /etc/hosts
09:40:57:      Ping to nsp_secondary OK
09:40:57:      nsp_oracle reflected in /etc/hosts
09:40:58:      Ping to nsp_oracle OK
09:40:58:      Oracle on nsp_oracle accessible
09:40:59: Analyzing disk usage
09:40:59:      Space not exceeded
09:41:00: Analyzing JMX agent properties
09:41:00:      Instance ID of JMX agent OK
09:41:01:      IxpMbean [ application type IXP+2 ] located
09:41:02: Checking syscheck - this can take a while
09:41:04:      No active alarms
09:41:05: Checking services
09:41:05:      NFS service is running
09:41:05:      Portmap service is running
09:41:06: Analyzing ssh keys
09:41:06:      Ping to ixp0907-1a OK
09:41:07:      Ping to ixp0907-1b OK
09:41:07:      Ping to ixp0907-1d OK
09:41:07:      Ping to ixp0907-1c OK
09:41:08:      All keys for cfguser accounts exchanged
09:41:08: Analyzing DaqServer table in IDB
09:41:09:      Server ixp0907-1a reflected in DaqServer table
09:41:09:      Server ixp0907-1b reflected in DaqServer table
09:41:10:      Server ixp0907-1d reflected in DaqServer table
09:41:11:      Server ixp0907-1c reflected in DaqServer table
09:41:13:      VIP is set in DaqSubSystem table
09:41:14:      VIP is set in HaVipDef table
09:41:14:      Ping to 10.250.70.115 OK
09:41:14:      VIP is accessible
09:41:15: Analyzing processes
09:41:28: >>> Warning: Process IxpOperate55919 restarted more then 5 times (29)
09:41:35: >>> Error: There are too many Dataflow processings (13). Should be 10
at most
09:41:35: >>> Suggestion: Dataflows should be redistributed to other servers
09:41:35:      Processes analysis done
09:41:36: Analyzing Data Feed status
09:41:37:      Data Feed analysis OK
09:41:37:      pdu_1 found in /etc/exports
09:41:38:      pdu_2 found in /etc/exports
09:41:38: Analyzing bulkconfig content
09:41:38:      BulkConfig content is consistent
09:41:39: All tests passed!
09:41:39: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp0907-1b

-----
ANALYSIS OF SERVER ixp0907-1c STARTED
-----

09:41:44: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
09:41:44: date: 05-17-15, hostname: ixp0907-1c
09:41:45: TPD VERSION: 7.0.1.0.0-86.20.0
09:41:45: IXP VERSION: [ 10.1.5.0.0-3.2.0 ]
09:41:46: XDR BUILDERS VERSION: [ 10.1.5.0.0-3.2.0 ]
09:41:46: -----
09:41:47: Analyzing server record in /etc/hosts
09:41:47:      Server ixp0907-1c properly reflected in /etc/hosts file
09:41:47: Analyzing IDB state
09:41:48:      IDB in START state
```

```

09:41:49: Analyzing shared memory settings
09:41:49:     Shared memory set properly
09:41:50: Analyzing IXP Licence
09:41:50:     Ixp Licence Valid
09:41:51: Analyzing date
09:41:51:     NTP daemon is running
09:41:52:     IP of NTP server is set
09:41:52: Checking CPU usage
09:41:52:     CPU usage check done
09:41:53: Running iaudit
09:41:54:     iaudit did not find any errors
09:41:55: Analyzing synchronization of server
09:41:56:     Role of server is Slave
09:41:57:     ActMaster server - ixp0907-1b
09:41:58:     StbMaster server - ixp0907-1a
09:41:59:     Server synchronizing properly
09:41:59: Analyzing NSP servers settings
09:41:59:     nsp_primary reflected in /etc/hosts
09:42:00:     Ping to nsp_primary OK
09:42:00:     nsp_secondary reflected in /etc/hosts
09:42:01:     Ping to nsp_secondary OK
09:42:01:     nsp_oracle reflected in /etc/hosts
09:42:01:     Ping to nsp_oracle OK
09:42:02:     Oracle on nsp_oracle accessible
09:42:02: Analyzing disk usage
09:42:03:     Space not exceeded
09:42:03: Analyzing JMX agent properties
09:42:03:     Instance ID of JMX agent OK
09:42:05:     IxpMbean [ application type IXP+2 ] located
09:42:05: Checking syscheck - this can take a while
09:42:08:     No active alarms
09:42:08: Analyzing ssh keys
09:42:09:     Ping to ixp0907-1a OK
09:42:09:     Ping to ixp0907-1b OK
09:42:09:     Ping to ixp0907-1c OK
09:42:10:     Ping to ixp0907-1d OK
09:42:10:     All keys for cfguser accounts exchanged
09:42:11: Analyzing DaqServer table in IDB
09:42:11:     Server ixp0907-1a reflected in DaqServer table
09:42:12:     Server ixp0907-1b reflected in DaqServer table
09:42:13:     Server ixp0907-1c reflected in DaqServer table
09:42:14:     Server ixp0907-1d reflected in DaqServer table
09:42:16:     VIP is set in DaqSubSystem table
09:42:16:     VIP is set in HaVipDef table
09:42:17:     Ping to 10.250.70.115 OK
09:42:17:     VIP is accessible
09:42:17: Analyzing processes
09:42:36: >>> Error: There are too many Dataflow processings (13). Should be 10
at most
09:42:37: >>> Suggestion: Dataflows should be redistributed to other servers
09:42:37:     Processes analysis done
09:42:37: Analyzing Data Feed status
09:42:39:     Data Feed analysis OK
09:42:39: Analyzing bulkconfig content
09:42:39:     BulkConfig content is consistent
09:42:40: All tests passed!
09:42:40: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp0907-1c

-----
ANALYSIS OF SERVER ixp0907-1d STARTED
-----

09:42:44: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0

```

PIC 10.1.5 Installation Guide

```
09:42:45: date: 05-17-15, hostname: ixp0907-1d
09:42:45: TPD VERSION: 7.0.1.0.0-86.20.0
09:42:46: IXP VERSION: [ 10.1.5.0.0-3.2.0 ]
09:42:46: XDR BUILDERS VERSION: [ 10.1.5.0.0-3.2.0 ]
09:42:47: -----
09:42:47: Analyzing server record in /etc/hosts
09:42:47:     Server ixp0907-1d properly reflected in /etc/hosts file
09:42:48: Analyzing IDB state
09:42:48:     IDB in START state
09:42:49: Analyzing shared memory settings
09:42:49:     Shared memory set properly
09:42:50: Analyzing IXP Licence
09:42:50:     Ixp Licence Valid
09:42:51: Analyzing date
09:42:51:     NTP daemon is running
09:42:52:     IP of NTP server is set
09:42:52: Checking CPU usage
09:42:52:     CPU usage check done
09:42:53: Running iaudit
09:42:54:     iaudit did not find any errors
09:42:55: Analyzing synchronization of server
09:42:56:     Role of server is Slave
09:42:56:     ActMaster server - ixp0907-1b
09:42:57:     StbMaster server - ixp0907-1a
09:42:58:     Server synchronizing properly
09:42:59: Analyzing NSP servers settings
09:42:59:     nsp_primary reflected in /etc/hosts
09:42:59:     Ping to nsp_primary OK
09:43:00:     nsp_secondary reflected in /etc/hosts
09:43:00:     Ping to nsp_secondary OK
09:43:00:     nsp_oracle reflected in /etc/hosts
09:43:01:     Ping to nsp_oracle OK
09:43:01:     Oracle on nsp_oracle accessible
09:43:02: Analyzing disk usage
09:43:02:     Space not exceeded
09:43:02: Analyzing JMX agent properties
09:43:03:     Instance ID of JMX agent OK
09:43:04:     IxpMbean [ application type IXP+2 ] located
09:43:05: Checking syscheck - this can take a while
09:43:07:     No active alarms
09:43:07: Analyzing ssh keys
09:43:08:     Ping to ixp0907-1a OK
09:43:08:     Ping to ixp0907-1b OK
09:43:08:     Ping to ixp0907-1d OK
09:43:09:     Ping to ixp0907-1c OK
09:43:09:     All keys for cfguser accounts exchanged
09:43:09: Analyzing DaqServer table in IDB
09:43:10:     Server ixp0907-1a reflected in DaqServer table
09:43:11:     Server ixp0907-1b reflected in DaqServer table
09:43:12:     Server ixp0907-1d reflected in DaqServer table
09:43:12:     Server ixp0907-1c reflected in DaqServer table
09:43:15:     VIP is set in DaqSubSystem table
09:43:15:     VIP is set in HaVipDef table
09:43:15:     Ping to 10.250.70.115 OK
09:43:16:     VIP is accessible
09:43:16: Analyzing processes
09:43:21:     Processes analysis done
09:43:22: Analyzing Data Feed status
09:43:23:     Data Feed analysis OK
09:43:23: Analyzing bulkconfig content
09:43:24:     BulkConfig content is consistent
09:43:24: All tests passed!
09:43:25: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp0907-1d
```

```
ixp0907-1a      TPD: [ 7.0.1.0.0-86.20.0 ]      IXP: [ 10.1.5.0.0-3.2.0 ]
XB: None      0 test(s) failed
ixp0907-1b      TPD: [ 7.0.1.0.0-86.20.0 ]      IXP: [ 10.1.5.0.0-3.2.0 ]
XB: [ 10.1.5.0.0-3.2.0 ]      0 test(s) failed
ixp0907-1c      TPD: [ 7.0.1.0.0-86.20.0 ]      IXP: [ 10.1.5.0.0-3.2.0 ]
XB: [ 10.1.5.0.0-3.2.0 ]      0 test(s) failed
ixp0907-1d      TPD: [ 7.0.1.0.0-86.20.0 ]      IXP: [ 10.1.5.0.0-3.2.0 ]
XB: [ 10.1.5.0.0-3.2.0 ]      0 test(s) failed
```

Example of a failed test:

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

9.9 Mediation Server Post-Integration Configuration (Optional)

This section contains various optional post-integration configuration procedures.

9.9.1 CSV streaming feeds and DataBroker

That procedure is to be followed to integrate a CSV server into an MEDIATION subsystem; such a server is used by the CSV streaming feed feature to store CSV files on a server that is not part of an MEDIATION subsystem.

This same procedure describes how to integrate a DataBroker server into an MEDIATION subsystem. Data Broker streaming feeds write files on customer servers providing NFS shared directories.

Note: For the CSV streaming feed feature, instead of using a dedicated server provided by the customer, it is possible to use a PDU server which is part of the current MEDIATION subsystem or which is part of another MEDIATION subsystem (as long as all the servers are in the same LAN).

Note: The following procedures describe how to setup shared directories using the NFS v3 protocol; it may be possible to use NFS v4, but the commands to execute are not described here (you should refer to linux and NFS documentation to learn how to use NFS v4 protocol).

1. Configure the shared directory on the sharing server

- a) Select an existing directory or already mounted local file system in which the exported files will be stored.

Note: Be sure the shared directory has read/write/execute access rights for MEDIATION's `cfguser` user. If the user `cfguser` also exists on the sharing server, with the same UID as on the MEDIATION servers, create the shared directory as `cfguser` (or mount the local file system in a directory owned by `cfguser`); in any other case, set RWX access rights on the shared directory for everybody.

- b) Update the exports file. As root, execute:

If the server uses a versioning system like `rcstool`, first check out the file:

```
# rcstool co /etc/exports
```

Edit `/etc/exports` and add this line (`<path_to_share>` is the directory or path to file system to share, `<ip_ixp_export>` is the IP address of an MEDIATION server); add as many lines as MEDIATION servers that will remotely access this shared directory

```
<path to share> <ip_ixp_export>(rw, sync, anonuid=-1)
```

If needed, check in the file:

```
# rcstool ci /etc/exports
```

PIC 10.1.5 Installation Guide

- c) Restart the NFS services. As root execute:

```
# chkconfig --levels 345 nfs on
# service rpcbind restart
# service nfs restart
```

2. Mount the shared directory on MEDIATION side

Note: These steps are to be executed on each MEDIATION server that will remotely access the shared directory of the sharing server.

- a) Create the mount point. As root, execute:

```
# mkdir /var/TKLC/ixp/StoreExport
# chown cfguser:cfg /var/TKLC/ixp/StoreExport
```

- b) Update the fstab file. As root, execute:

```
# rcstool co /etc/fstab
```

Edit /etc/fstab and add this line (<ip_server_nfs> is the IP address of the sharing server)

```
<ip_server_nfs>:<path_to_share> /var/TKLC/ixp/StoreExport nfs
rw,rsize=32768,wsiz=32768,soft 0 0
```

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

```
# mount --all
```

- c) Restart the NFS services. As root execute:

```
# chkconfig --levels 345 nfs on
# service rpcbind restart
# service nfs restart
```

Note: The firewall must be disabled on the shared CSV server. If the CSV server is maintained by Oracle(Tekelec) then following steps must be performed to disable the firewall as root user

- a) `chkconfig --levels 345 iptables off`
- b) `service iptables stop`

If the CSV server is not maintained by Oracle then firewall must be disabled or configured to allow the nfs connections.

9.9.2 Delivery Network Failure and Recovery (DataBroker)

This application shall be available 24 hours a day, seven days per week, except for minimal downtime due to planned production maintenance.

Note: Even if this procedure is applicable to all the MEDIATION servers, it is not recommended to apply it for other purposes than DataBroker streaming feed, for which only it has been tested.

1. Configure IDB to extend 24 hours of xDRs can be kept in the DTS buffers

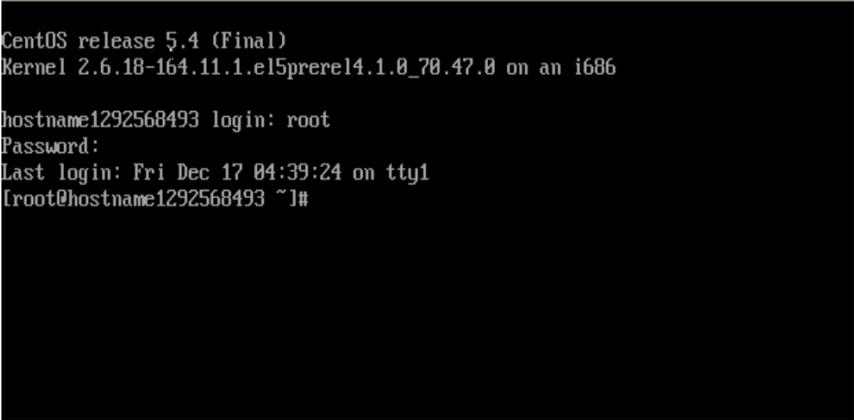
As cfguser on MEDIATION primary , run:

```
# IxpExtendDataBroker24hrs.sh
```

Result with 3 MEDIATION servers:

```
Testing host is primary .....
Host is primary
Testing user is cfguser .....
User is cfguser
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1b    ===
changed 1 records ===
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1c    ===
changed 1 records ===
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1a    ===
changed 1 records ===
```


10 APPENDIX: MANUAL CONFIGURATION OF ETHERNET INTERFACES

S T E P #	<p>In this section you will be configuring the Ethernet interfaces in preparation to test them. You will be configuring the IP address, Netmask, Gateway for the interfaces on each TPD HP based server. If the final customer network and IP address information is not available at the time of this configuration, a default IP address for each server should be provided.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> - The servers are loaded with TPD - The HP ProLiant servers will need to be connected to a KVM for access. <p>Notes: Within the Platform Configuration Utility, the arrow and Tab keys on your keyboard can be used to move the cursor to different fields.</p>	
1	<p>Login to the server</p>	<p>Once the server completes the reboot from the ILO configuration process in the previous section, you should see a login prompt.</p> <p>Login as User: root and refer to TR006061 for the default “TPD root” password</p>  <pre>CentOS release 5.4 (Final) Kernel 2.6.18-164.11.1.el5pre.el4.1.0_70.47.0 on an i686 hostname1292568493 login: root Password: Last login: Fri Dec 17 04:39:24 on tty1 [root@hostname1292568493 ~]#</pre> <p>Expected Result: Login prompt is displayed and you are logged in as root.</p>

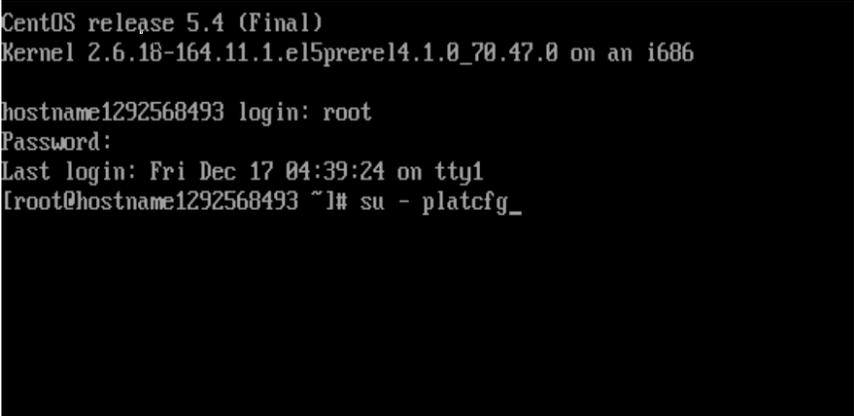
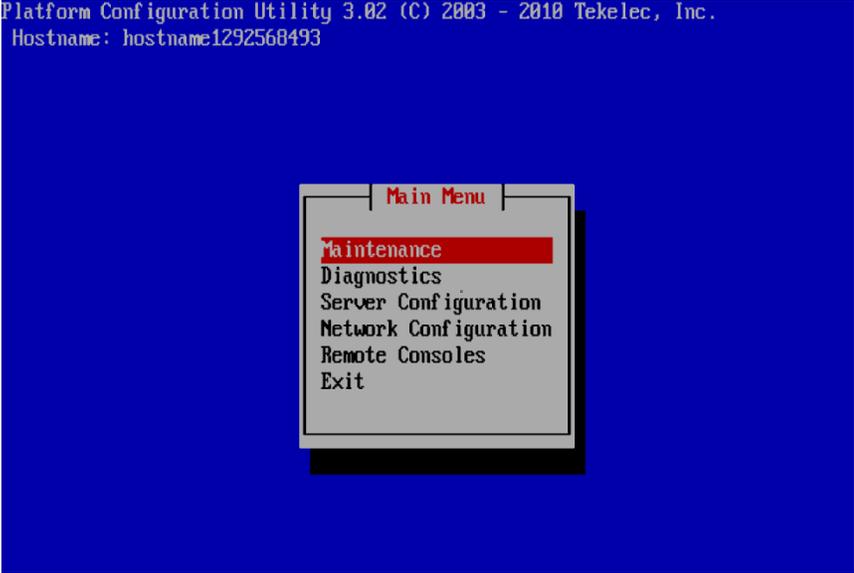
1. Using command line procedure

If you Prefer to configure using the graphical interface skip this procedure and use the following platcfg menu procedure

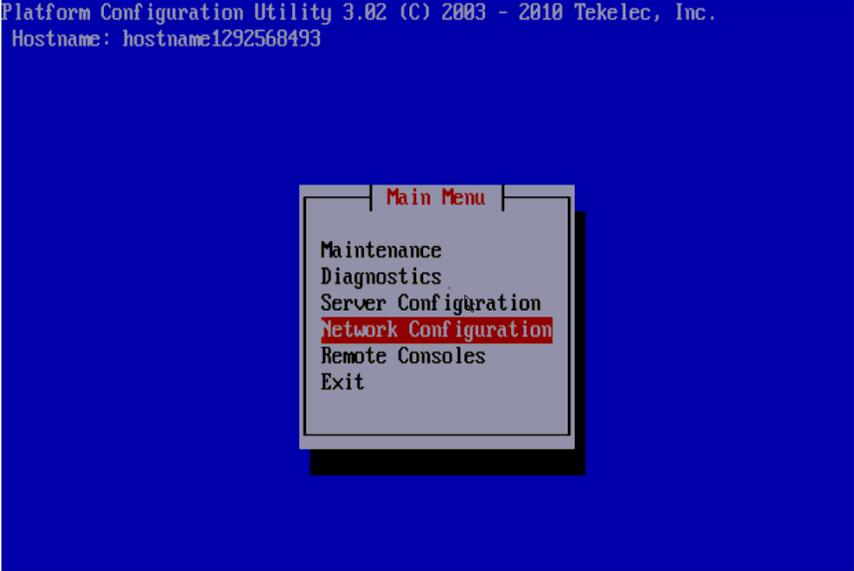
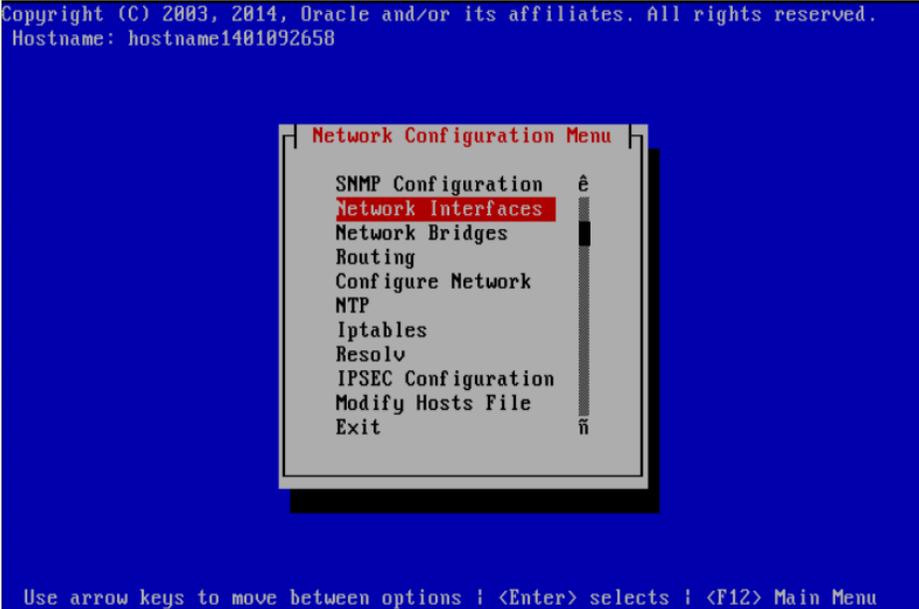
2	<p>Set the IP address and Netmask identified for the eth01 interface</p>	<p>Command:</p> <pre># ifconfig eth01 <CUST IP ADDRESS> netmask <MASK> #</pre> <p>Expected Result: No error after executing the command</p>
3	<p>Set the default Route Gateway IP address for the eth01 interface</p>	<p>Command:</p> <pre># route add default gw <DEFAULT ROUTE IP ADDRESS> #</pre> <p>Expected Result: No error after executing the command</p>
4	<p>Configure remaining servers in frame</p>	<p>Repeat Steps 1 through 3 for each equipped HP server.</p>

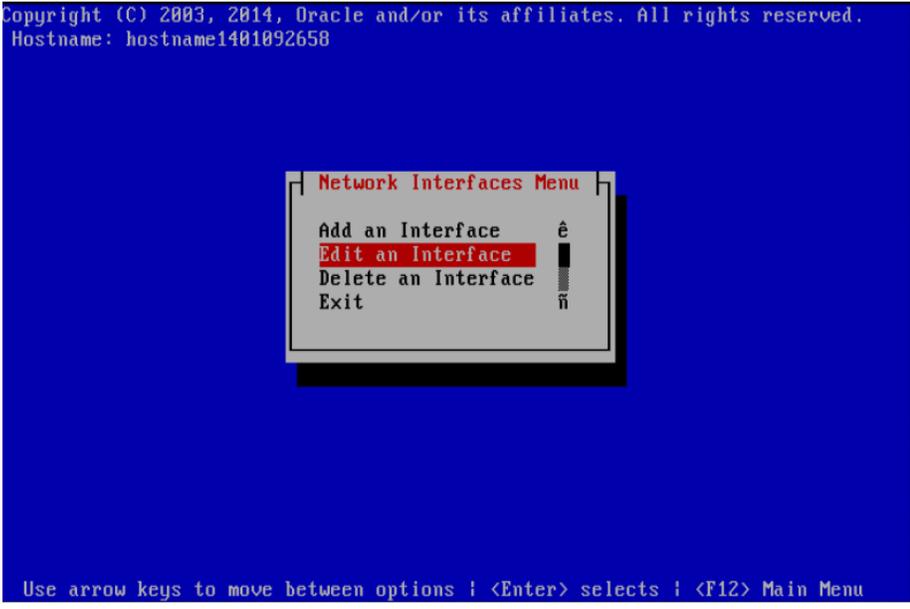
2. Using platcfg menu procedure

If you configure IP using the command line following the previous procedure, you can skip this procedure as it is already completed.

2	Enter the Platform Configuration Utility	<p>To enter the Platform Configuration Utility menu enter: <code>su - platcfg</code></p> 
3	Enter the Platform Configuration Utility	<p>Platform Configuration Utility 3.02 (C) 2003 - 2010 Tekelec, Inc. Hostname: hostname1292568493</p>  <p>Expected Result: Main Menu of Platform Configuration Utility is displayed</p>

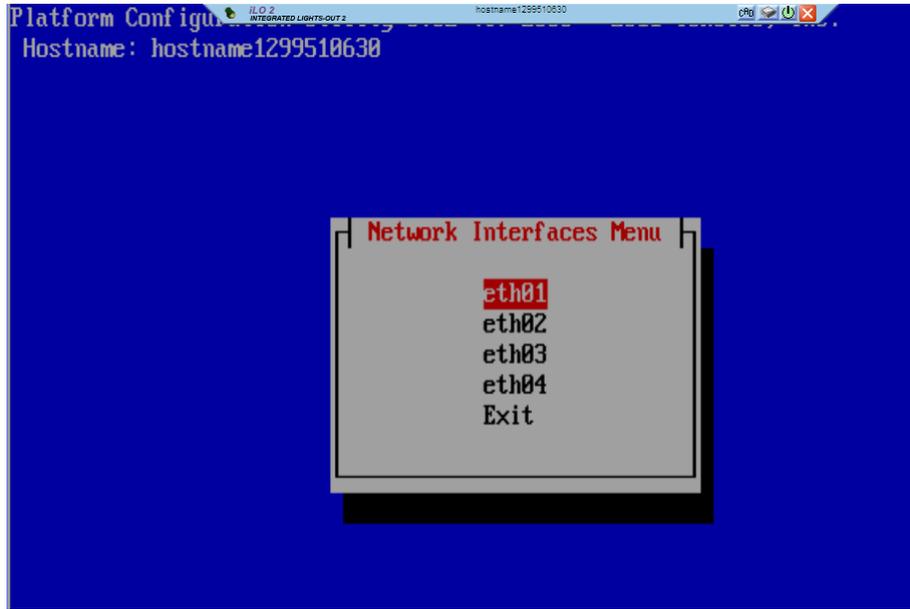
PIC 10.1.5 Installation Guide

<p>4</p>	<p>Enter the Network Configuration menu of the Platform Configuration Utility</p>	<p>Main Menu of Platform Configuration Utility is displayed. Use the arrow keys on the keyboard to select Network Configuration and press [ENTER] to select it.</p>  <p>Expected Result: The Network Configuration menu is displayed</p>
<p>5</p>	<p>Enter the Network Interfaces menu</p>	<p>Use the arrow keys on the keyboard to select Network Interfaces and press [ENTER] to select it.</p>  <p>Expected Result: The Network Interfaces menu is displayed</p>

<p>6</p>	<p>Enter the Edit an Interface menu</p>	<p>Use the arrow keys on the keyboard to select Edit an Interface and press [ENTER] to select it.</p>  <p>Expected Result: The Network Interfaces menu is displayed with interface choices eth01 and eth02</p>
----------	---	--

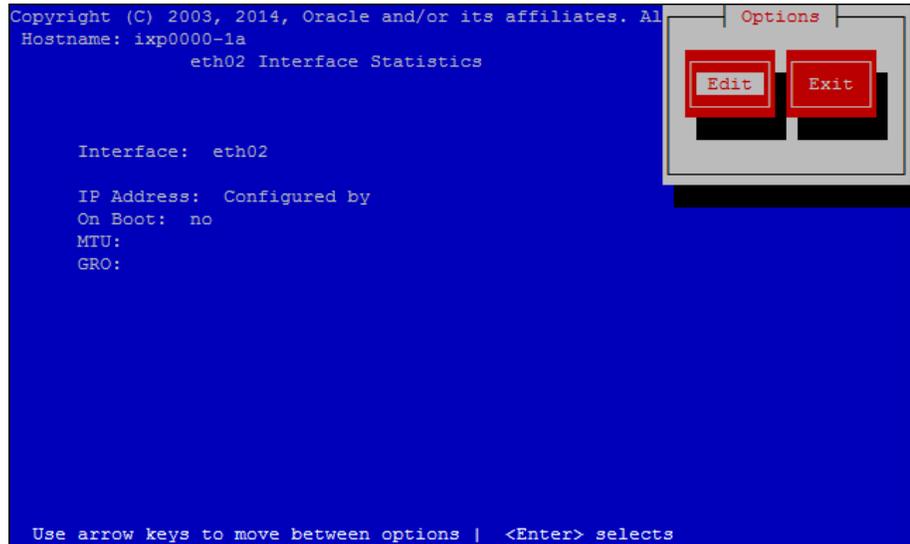
7 Edit the eth01 interface properties

Use the arrow keys on the keyboard to select **eth01** and press **[ENTER]** to select it.



Expected Result:

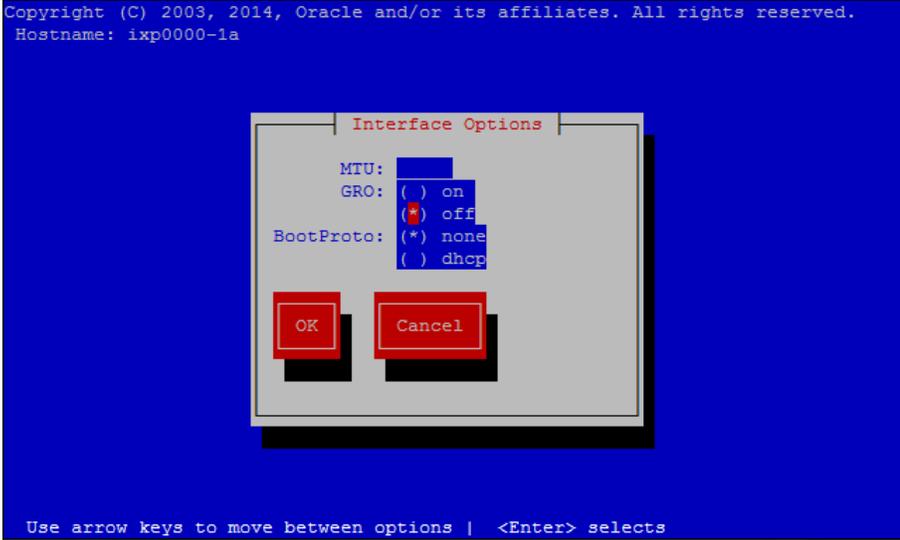
The eth01 interface is selected and you are presented with **eth01 Interface Statistics**.



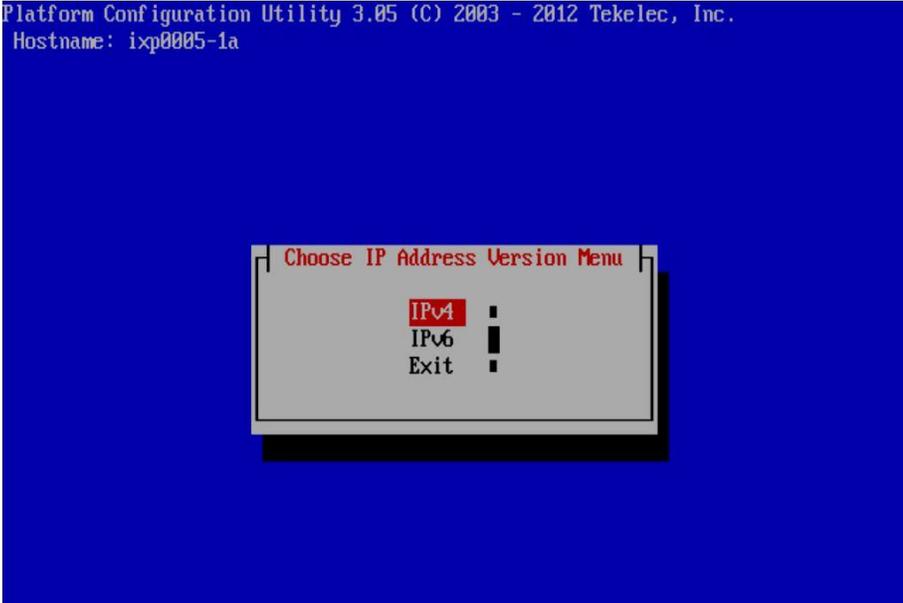
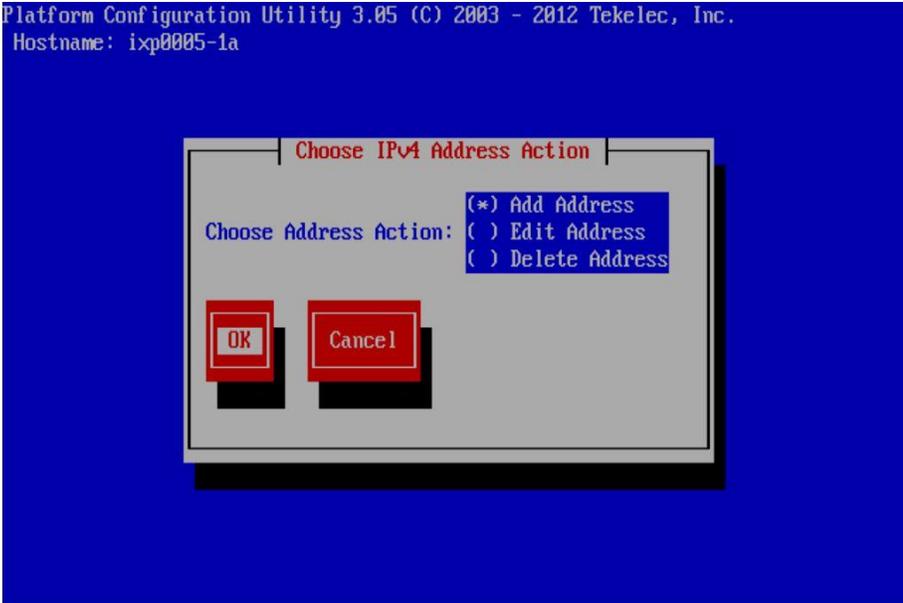
Press the **[ENTER]** key to Edit the properties of eth01.

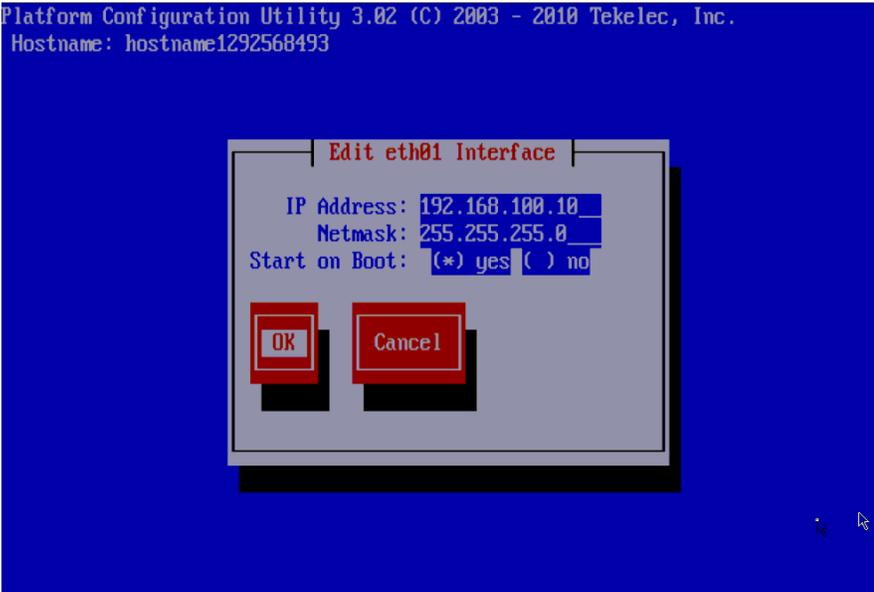
Expected Result:

The eth01 interface is selected and you are presented with eth01 Interface Statistics. You have selected 'Edit' and are presented with properties to change.

<p>8</p>	<p>Configure MTU, GRO, and boot protocol</p>	<p>Press [TAB] to move to off for GRO, then press the [SPACEBAR] key to select it. An asterisk will appear once selected.</p> <p>Press [TAB] to move to OK, then press the [ENTER] key to continue.</p>  <p>Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved. Hostname: ixp0000-1a</p> <p>Interface Options</p> <p>MTU: <input type="text"/></p> <p>GRO: () on (*) off</p> <p>BootProto: (*) none () dhcp</p> <p>OK Cancel</p> <p>Use arrow keys to move between options <Enter> selects</p> <p>Expected Result: GRO is set to off and you now see the menu which allows you to edit the IP address.</p>
<p>9</p>	<p>Configure IP</p>	<p>Press [TAB] to move to Yes, then press the [ENTER] key to continue.</p>  <p>Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved. Hostname: ixp0000-1a</p> <p>Configure IP Address</p> <p>Would you like to configure IP addresses?</p> <p>No Yes</p> <p>Use arrow keys to move between options <Enter> selects</p>

PIC 10.1.5 Installation Guide

10	Select IPv4	<p>press [ENTER] to continue.</p>  <p>Platform Configuration Utility 3.05 (C) 2003 - 2012 Tekelec, Inc. Hostname: ixp0005-1a</p> <p>Choose IP Address Version Menu</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> IPv4<input type="checkbox"/> IPv6<input type="checkbox"/> Exit
11	Select Add address	<p>press [ENTER] to continue.</p>  <p>Platform Configuration Utility 3.05 (C) 2003 - 2012 Tekelec, Inc. Hostname: ixp0005-1a</p> <p>Choose IPv4 Address Action</p> <p>Choose Address Action:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Add Address<input type="checkbox"/> Edit Address<input type="checkbox"/> Delete Address <p>OK Cancel</p>

<p>12</p>	<p>Set the IP address and Netmask identified for the eth01 interface</p>	<p>Use the [TAB] and arrow keys on the keyboard to add IP address. Enter the IP address of the server then press [TAB] to select NETMASK. Press [TAB] to select () yes and press [SPACEBAR] to select then [TAB] and press [ENTER] to continue.</p> 
<p>13</p>		<p>You will see the following screen:</p>  <p>Expected Result: IP address and Netmask is set to the correct IP address for the server. Wait for it to complete.</p>

PIC 10.1.5 Installation Guide

14 Verify the settings and exit

Once the screen comes back, **verify the IP address and Netmask**. Use the **[TAB]** key on the keyboard to select Exit and press **[ENTER]** to continue.

```
Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved.  
Hostname: ixp0000-1a  
eth01 Interface Statistics  
  
Interface: eth01  
IP Address: 10.31.8.23  
Netmask: 255.255.255.0  
On Boot: yes  
MTU:  
GRO: off
```



Use arrow keys to move between options | <Enter> selects

Use the **[TAB]** key on the keyboard to select Exit and press **[ENTER]** to continue

```
Platform Configuration Utility 3.02 (C) 2003 - 2010 Tekelec, Inc.  
Hostname: hostname1292568493
```



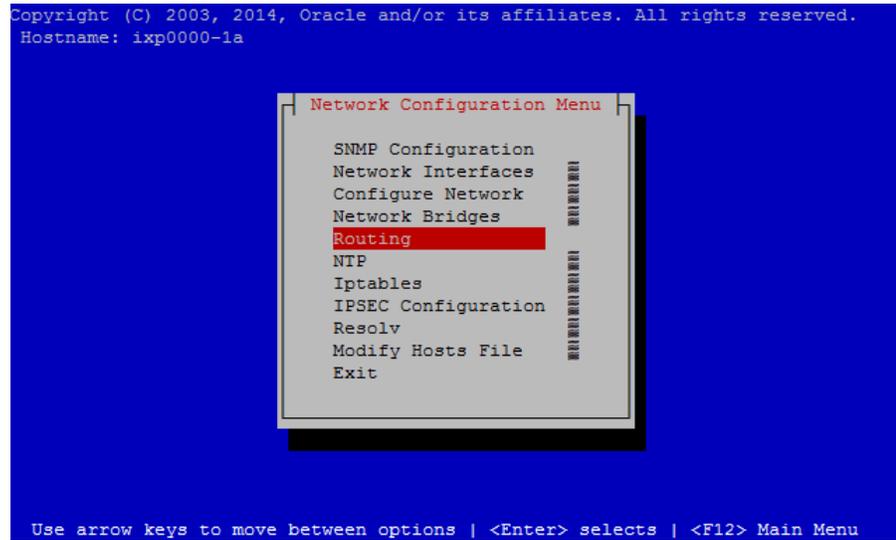
```
Network Interfaces Menu  
Add an Interface  
Delete an Interface  
Edit an Interface  
Exit
```

Expected Result:

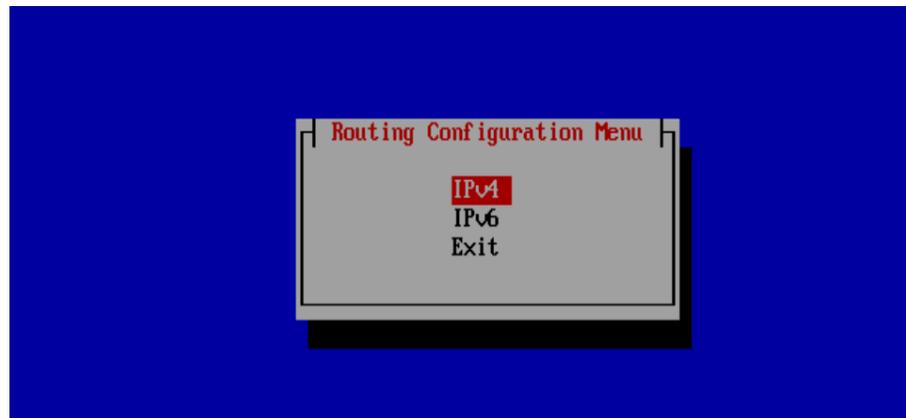
IP address and Netmask is set to the correct IP address for the server and you exit the Network Interfaces menu.

15 Set the Gateway address for the eth01 interface

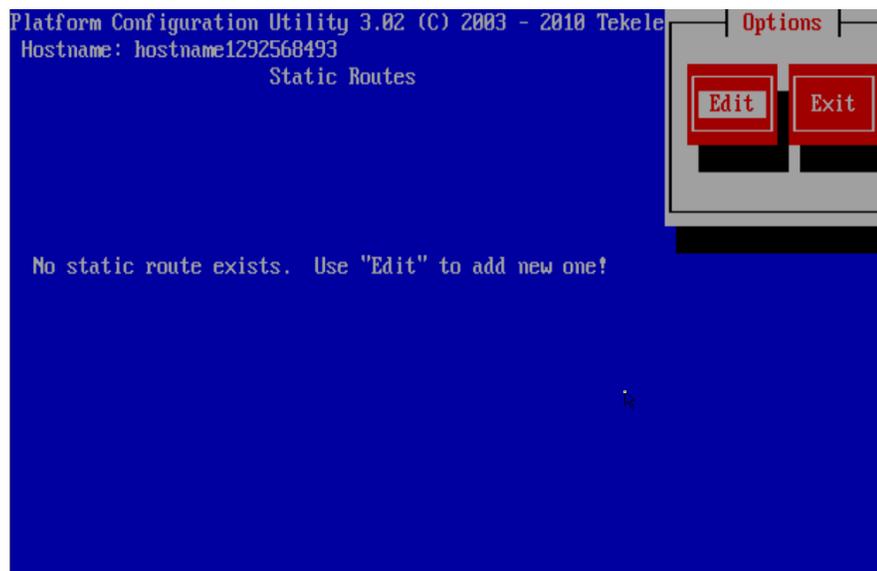
Use the arrow keys on the keyboard to select Routing and press **[ENTER]** to continue.



Select IPv4 and press **[ENTER]** to continue.



Select Edit and press **[ENTER]** to add the default gateway.

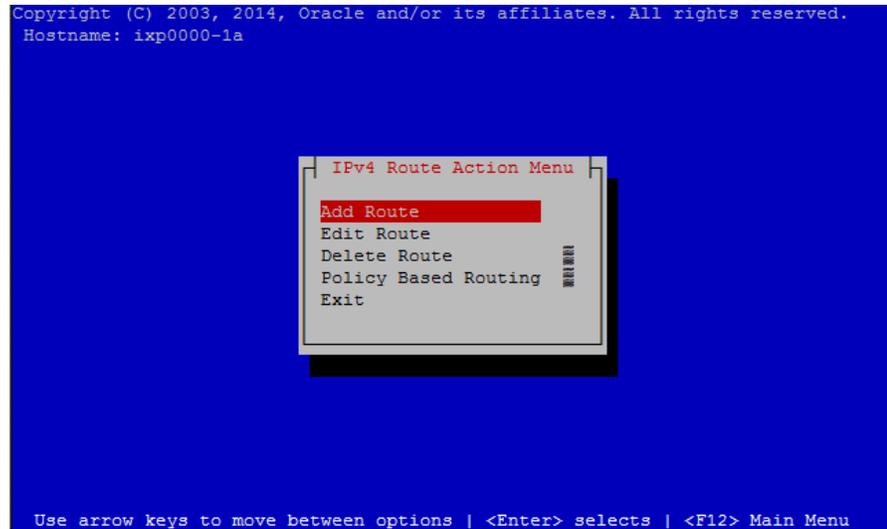


Expected Result:
 Routing menu is opened and Edit is selected

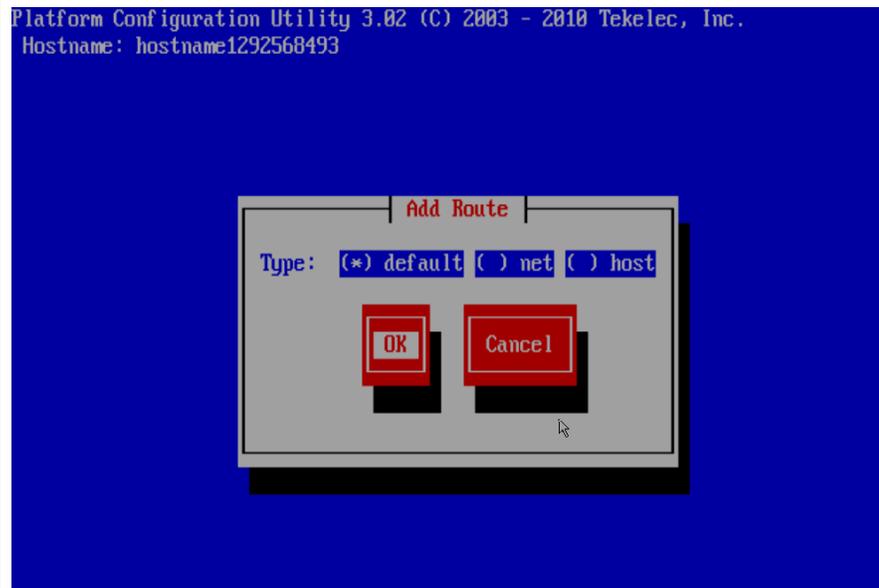
PIC 10.1.5 Installation Guide

16 Set the IP address and Netmask for the eth01 interface

Select Add Route using the arrow keys.

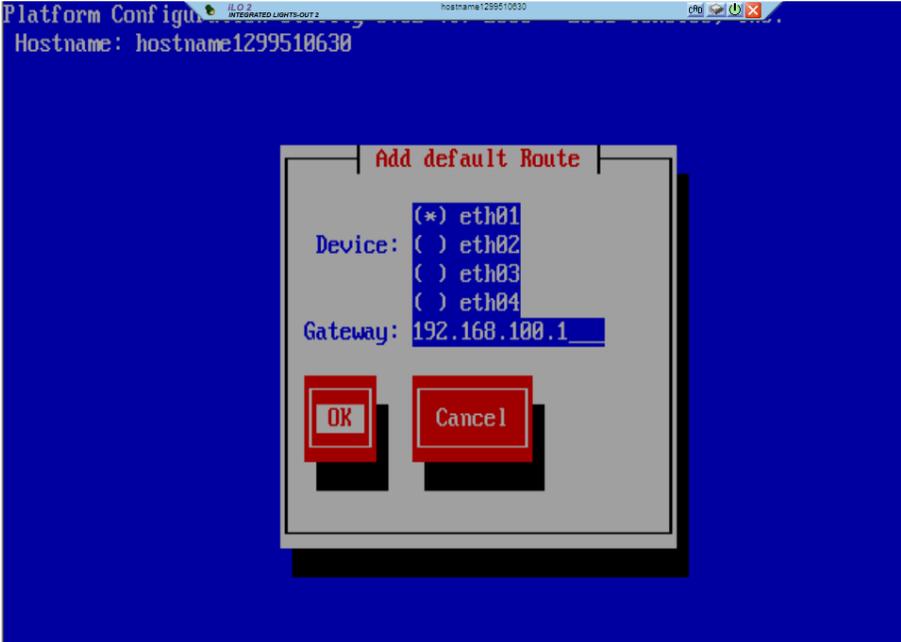
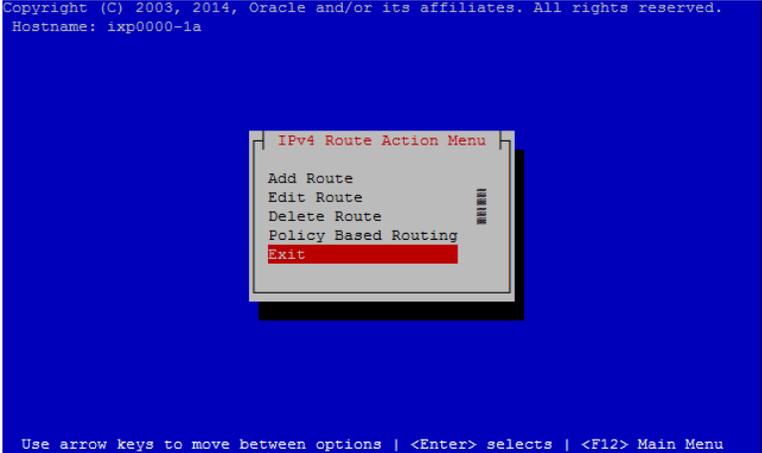


Use the [TAB] and [SPACEBAR] keys on the keyboard to select () **default**, then [TAB] to **OK** and press [ENTER] to continue.



Expected Result:

Default is selected and you are taken to the next menu which allows you to add the IP address of the default route.

<p>17</p>	<p>Set the default Route Gateway IP address for the eth01 interface</p>	<p>Use the [TAB] and [SPACEBAR] keys on the keyboard to select (*) eth01 and then [TAB] twice and enter the correct customer's gateway IP address if available. If not available and you are using default test IP addresses instead, enter 192.168.100.1. Press [TAB] to select OK then press [ENTER] to continue.</p>  <p>Use the arrow keys on the keyboard to select Exit then press [ENTER] to exit.</p>  <p>Expected Result: The correct Gateway IP address is entered. The Route Action menu is exited.</p>
<p>18</p>	<p>Verify the default Route for eth01 and exit the menu</p>	<p>Verify the eth01 interface is listed and Type and Address are set to default. Gateway should match the IP address you entered in the previous step. Use the [TAB] key on the keyboard to select Exit and press [ENTER] to continue.</p>

PIC 10.1.5 Installation Guide

```
Platform Configuration Utility 3.02 (C) 2003 - 2010 Tekelec
Hostname: hostname1292568493
Static Routes

Interface  Type  Address  Netmask  Gateway
-----  -
eth01     default  default  -----  192.168.100.1

Options
Edit  Exit
```

Select **Exit** and press **[ENTER]** to leave the **Routing Configuration** menu

```
Routing Configuration Menu
IPV4
IPV6
Exit
```

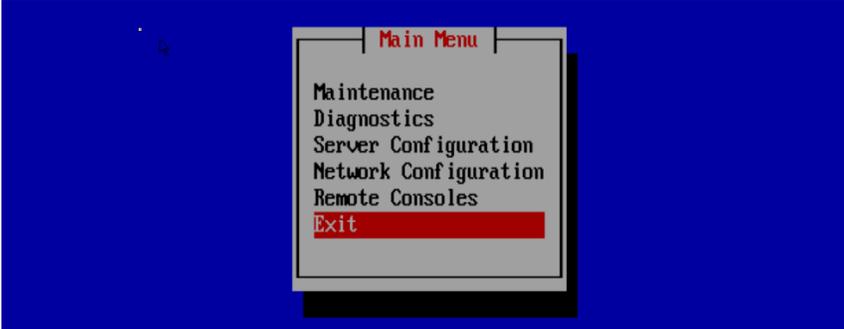
Select **Exit** and press **[ENTER]** to leave the **Network Configuration** menu

```
Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved.
Hostname: ixp0000-1a

Network Configuration Menu
SNMP Configuration
Network Interfaces
Configure Network
Network Bridges
Routing
NTP
Iptables
IPSEC Configuration
Resolve
Modify Hosts File
Exit

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

Select **Exit** once again to leave the **Platform Configuration Utility**

		 <p>Expected Result: The default route (Gateway) IP address is verified and the menu is exited.</p>
19	Configure remaining servers in frame	Repeat Steps 1 through 18 for each equipped HP DL360 server.

11 APPENDIX: PIC BULKCONFIG FILE DESCRIPTION

11.1 Management Server Bulkconfig File Description

Note: ON ODA no bulkconfig file is required

The MANAGEMENT SERVER subsystem bulkconfig file contains the overall Management Server pre-installation configuration information, most importantly the hostname and SNMP configuration. During the installation process,

various scripts use this file to configure Management Server.

The bulkconfig file is a text file and as such can be created or updated with any available text editor,

e.g. vi or vim.

The bulkconfig file templates can be found on the Management Server iso in the / directory. For Management Server One-Box you

can use the /bulkconfig.nsp-onebox template together with the /bulkconfig.example.nsp-onebox example showing an updated bulkconfig template. Do not use this reference example to configure the Management Server system. For Management Server Four-Box you can use the /bulkconfig.nsp-fourbox template together with the /bulkconfig.example.nsp-fourbox example.

Note: When you install PIC, you are asked to create this bulkconfig file and update this file. DO NOT remove the Management Server bulkconfig file from the server.

This topic provides a description of each keyword and parameter used in the bulkconfig file. It is important to read and understand the contents of this file.

bulkconfig file location and rights

File name: bulkconfig

File absolute path: /root/bulkconfig

Mount the Management Server iso file. As root run :

```
# mount -o loop /var/TKLC/upgrade/iso_file.iso /mnt/upgrade
```

Copy the good bulkconfig file template:

For one Box

```
# cp /mnt/upgrade/bulkconfig.nsp-onebox /root/bulkconfig
```

For four Box

```
# cp /mnt/upgrade/bulkconfig.nsp-fourbox /root/bulkconfig
```

Change the permission on the bulkconfig

```
# chmod 644 /root/bulkconfig
```

Unmount the Management Server iso file. As root run :

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

bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword, and then contains various values for

this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_gateway
ntpserver1,IP_address
ntpserver2,IP_address
timezone,time_zone
```

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

host Description

```
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_gateway
```

...

The host keyword has the following associated values:

<i>hostname_of_server</i>	A valid hostname , it should match the hostname set on server.
<i>The IP address of the server.</i>	For blade systems, the internal IP address of the server.
<i>IP_address</i> of	The IP address of the server. For blade systems, the internal IP address of the server.
<i>function</i>	The function of the server. Use one of the following entries: <ul style="list-style-type: none"> • NSP_ONEBOX for the Management Server One-box Server • NSP_APACHE for the Management Server Apache Server • NSP_ORACLE for the Management Server Oracle Server • NSP_SECONDARY for the Management Server Secondary Server • NSP_PRIMARY for the Management Server Primary Server
<i>interface_name</i>	Name of the interface where the network settings are applied. <ul style="list-style-type: none"> • Use eth01 (backend) for a rackmount system and eth02 (frontend)for the second interface on Apache and One-box servers. • Use bond0.3 for the blade systems and bond0.4 for the second interface on Apache and One-box servers.
<i>network_mask</i> <i>network_gateway</i>	The network mask. The default gateway On Apache and One-box servers the gateway <u>must be the one from frontend</u> (eth02) for all interfaces including the backend interface (eth01) on apache server (frontend gateway must be put on bot lines)



In the case some Mediation/Acquisition servers are not on the same subnetwork as Management Server backend, routes to thoses subnetworks must be manually added in Management Server, specifying as gateway the interface matching the physical customer network topology (backend or frontend). Use platcfg tool to add those routes.

ntpserver Description

Refer to Appendix 17 to know how to configure NTP.

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

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

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server

timezone Description

```
timezone,time_zone
```

PIC 10.1.5 Installation Guide

The timezone keyword has the following associated value:

time_zone

The timezone string. For a list of available timezones that you can use, refer to the /usr/share/zoneinfo/zone.tab file TZ column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
time_zone
--CUT--
#code coordinates TZ comments
AD +4230+00131 Europe/Andorra
AE +2518+05518 Asia/Dubai
AF +3431+06912 Asia/Kabul
AG +1703-06148 America/Antigua
CZ +5005+01426 Europe/Prague
---CUT---
```

Management Server One-box

bulkconfig Template

```
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_gateway
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_gateway
ntpserver1,IP_address
ntpserver2,IP_address
timezone,time_zone
```

Example:

A bulkconfig file needs to be created for the Management Server One-box:

- Server hostname: nsp-onebox
- Because it is a one-box server, two interfaces are needed
- Because it is a rackmount system, use eth01 and eth02 for these interfaces

Note: If you are configuring C-class blades, replace eth01 with bond0.3 and eth02 with bond0.4 when you create this file.

- IP addresses:
 - First interface (eth01): 10.236.2.141
 - Second interface (eth02): 10.236.1.141
- Subnet mask: 255.255.255.254
- Gateway addresses:
 - First interface (eth01): 10.236.2.129
 - Second interface (eth02): 10.236.1.129
- NTP server IP address: 10.236.129.11
- Server timezone: Europe/Paris

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@nsp-onebox ~]# cat /root/bulkconfig
host,nsp-onebox,10.236.2.141,NSP_ONEBOX,eth01,255.255.255.224,10.236.1.129
host,nsp-onebox,10.236.1.142,NSP_ONEBOX,eth02,255.255.255.224,10.236.1.129
ntpserver1,10.236.129.11
ntpserver2,
timezone,Europe/Paris
```

Note: in case there is no network connectivity from backend gateway to frontend IP, the frontend line must be removed from bulkconfig file, and interface must be configured manually using platcfg tool.

11.2 Mediation Server Bulkconfig File Description

The MEDIATION subsystem bulkconfig file contains the overall MEDIATION pre-installation configuration information.

Note: there is one bulkconfig file for each MEDIATION subsystem.

During the installation process, various scripts use this file to configure MEDIATION.

The bulkconfig file is a case sensitive text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The MEDIATION bulkconfig file template is located on the MEDIATION iso on the /upgrade/IXP_bulkconfig_template path. The file is unique for the MEDIATION subsystem and is present on each server in this subsystem.

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

The MEDIATION subsystem bulkconfig file is used during these processes:

- Manufacturing installation
- Customer network integration
- Change IP
- Disaster recovery procedure

This topic provides a description of each keyword and parameter used in the bulkconfig file. It is important to read and understand the contents of this file.

bulkconfig file location and rights

File name: bulkconfig

File absolute path: /root/bulkconfig

Mount the Mediation iso file. As root run :

```
# mount -o loop /var/TKLC/upgrade/iso_file.iso /mnt/upgrade
```

Copy the good bulkconfig file template:

```
# cp /mnt/upgrade/upgrade/IXP_bulkconfig_template /root/bulkconfig
```

Change the permission on the bulkconfig

```
# chmod 644 /root/bulkconfig
```

Unmount the MEDIATION iso file. As root run :

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

bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The

PIC 10.1.5 Installation Guide

keyword is mandatory. Each line must begin with the keyword, and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_1st_server,IP_address,function,interface_name,network_mask,network_gateway
host,hostname_of_2nd_server,IP_address,function,interface_name,network_mask,network_gateway
host,hostname_of_nth_server,IP_address,function,interface_name,network_mask,network_gateway
ntpserver1,IP_address
ntpserver2,IP_address
ntpserver3,IP_address
ntppeerA,
ntppeerB,
nspprimary,IP_address_of_primary_weblogic_or_onebox_nsp_backend
nspsecondary,IP_address_of_secondary_weblogic
nsporacle,IP_address_of_oracle_server
timezone,time_zone
pdu,IP_address,directory_path
pdu,IP_address,directory_path
```

The highlighted entries are for the PDU share directories on external storage server like ZFS

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

host Description

```
host,hostname_of_1st_server,IP_address,function,interface_name,network_mask,network_gateway
host,hostname_of_2nd_server,IP_address,function,interface_name,network_mask,network_gateway
host,hostname_of_nth_server,IP_address,function,interface_name,network_mask,network_gateway
```

...

Example (installation):

```
host,ixp1981-1a,10.236.2.141,IXP-PDU,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,IXP-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-BASE,eth01,255.255.255.224,10.236.2.129
```

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

Example (disaster recovery of ixp1981-1b server):

```
host,ixp1981-1a,10.236.2.141,IXP-PDU,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,DR-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-BASE,eth01,255.255.255.224,10.236.2.129
```

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

The host keyword has the following associated values:

hostname_of_nth_server The server hostname in the standard MEDIATION format: ixpNNNN-MA where:

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

IP_address The IP address of the server. For blade systems, the backend (VLAN 3) IP address of the server.

function The function of the server. Use one of the following entries for installation:

- IXP-PDU for the PDU Storage Server
- IXP-BASE for the IXP Base Server

Function for the disaster recovery procedure for the particular server is different. Use one of the following entries for disaster recovery:

- DR-PDU for the PDU Storage Server
- DR-BASE for the IXP Base Server

interface_name Name of the interface where the network settings are applied.

- eth01 for the rackmount systems
- bond0.3 for the blade systems

network_mask The network mask.

network_gateway The default gateway.

ntpserver Description

Refer to Appendix 17 to know how to configure NTP.

```
ntpserver1,IP_address
ntpserver2,IP_address
ntpserver3,IP_address
ntppeerA,
ntppeerB,
```

- ntpserver1 is the first NTP server
- ntpserver2 is the second NTP server
- ntpserver3 is the third NTP server
- ntppeerA not applicable; leave empty
- ntppeerB not applicable; leave empty

Example:

```
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
```

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server.

NSP Description

nspprimary,IP_address_of_primary_weblogic_or_onebox_nsp_backend_or_IP_address_of_managedServer1_on_ODA

nspssecondary,IP_address_of_secondary_weblogic_or_IP_address_of_managedServer2_on_ODA

nsporacle,IP_address_of_oracle_server_or_oda_base_IP_address

PIC 10.1.5 Installation Guide

`nspadmin,IP_address_of_admin_server_oda`

- `nspprimary` is the Management Primary WebLogic server or the One-box Management server or the managed server1 on ODA
- `nspsecondary` is the Management Secondary WebLogic server or the managed server2 on ODA
- `nsporacle` is the Management Oracle server or ODA_BASE
- `nspadmin` is the Management Weblogic Admin Server on ODA

Note: The `nspadmin` entry is only needed when the Management server is installed on ODA. In case of ODA, `nspprimary` server shall depict `weblogic managed server1` and `nspsecondary` server shall depict `weblogic managed server2`

Example (for a One-box Management Server):

```
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
```

The NSP keyword has the following associated values:

IP_address_of_primary_weblogic_or_onebox_nsp_backend The IP address of the MANAGEMENT SERVER server:

- One-box: backend IP address of the One-box Management Server

IP_address_of_secondary_weblogic The IP address of the Management Server:

- One-box: not applicable; leave empty

IP_address_of_oracle_server The IP address of the Management Server Oracle server:

- One-box: not applicable; leave empty

Example (For ODA based Management Server):

```
nspprimary,10.10.10.11
nspsecondary,10.10.10.12
nsporacle,10.10.10.9
nspadmin,10.10.10.10
```

The NSP keyword has the following associated values:

IP_address_of_weblogic_managed_server1_on_ODA

IP_address_of_weblogic_managed_server2_on_ODA

IP_address_of_oracle_server_on_ODA

IP address of weblogic admin server on ODA

timezone Description

`timezone,time_zone`

Example:

```
timezone,Europe/Paris
```

The `timezone` keyword has the following associated value:

time_zone

The `timezone` string. For a list of available timezones that you can use, refer to the `/usr/share/zoneinfo/zone.tab` file TZ column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT--
#code coordinates TZ comments
AD +4230+00131 Europe/Andorra
909-2122-001 Revision 1.11, February 02, 2012 DRAFT 210
PIC Bulkconfig File Description
AE +2518+05518 Asia/Dubai
AF +3431+06912 Asia/Kabul
AG +1703-06148 America/Antigua
CZ +5005+01426 Europe/Paris
--CUT--
```

bulkconfig file: installation example

A bulkconfig file needs to be created for the following MEDIATION subsystem:

- Subsystem hostname: ixp1981
- 1a server is the PDU Storage Server with the IP address: 10.236.2.141
- 1b server is the Base Server with the IP address: 10.236.2.142
- 1c server is the Base Server with the IP address: 10.236.2.143
- Network interface: eth01
- Network mask: 255.255.255.254
- Default gateway: 10.236.2.129
- NTP server IP address: 10.236.129.11
- NSP One-box IP address: 10.10.10.10
- Server timezone: Europe/Paris

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@ixp1981-1a ~]# cat /root/bulkconfig
host,ixp1981-1a,10.236.2.141,IXP-PDU,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,IXP-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-BASE,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
timezone,Europe/Paris
```

Automated records in /etc/bulkconfig file

During the automated integration of MEDIATION subsystem with EFS server(s) the following line is added to

the /etc/bulkconfig file (one per integrated EFS server):

```
efs,hostname_of_EFS,IP_address_of_EFS
```

PIC 10.1.5 Installation Guide

where

- `hostname_of_EFS` is the hostname of EFS that local DataFeeds hosts uses as an export target
- `IP_address_of_EFS` is the IP address of such EFS

Example:

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

External PDU storage server Description

After mediation server installation and before customer integration the following lines should be added in `bulkconfig` to add the mounts on external storage server for PDU storage.

```
pdu,IP_address,directory_path  
pdu,IP_address,directory_path
```

- `pdu` is the keyword to identify the external pdu storage server entry.
- `IP_address` is the ip address of the external PDU storage server.
- `directory_path` is the path of directory on external PDU storage server to be mounted on mediation server to store the PDUs

Example for ZFS storage server :

```
pdu,10.31.2.72,/export/pdu_1  
pdu,10.31.2.72,/export/pdu_2  
pdu,10.31.2.75,/export/pdu_1  
pdu,10.31.2.75,/export/pdu_3
```

11.3 DWS Bulkconfig File Description

The DWS `bulkconfig` file contains the overall DWS pre-installation configuration information.

During the installation process, various scripts use this file to configure the DWS.

The `bulkconfig` file is a case sensitive text file and as such can be created or updated with any available text editor, e.g. `vi` or `vim`.

The DWS `bulkconfig` file template is located on the MEDIATION iso on the `/upgrade/IXP_bulkconfig_template` path. The file is unique for each DWS.

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

The DWS `bulkconfig` file is used during these processes:

- Manufacturing installation
- Customer network integration
- Change IP
- Disaster recovery procedure

This topic provides a description of each keyword and parameter used in the `bulkconfig` file. It is important to read and understand the contents of this file.

bulkconfig file location and rights

File name: `bulkconfig`

File absolute path: /root/bulkconfig

Mount the MEDIATION iso file. As root run :

```
# mount -o loop /var/TKLC/upgrade/iso_file.iso /mnt/upgrade
```

Copy the good bulkconfig file template:

```
# cp /mnt/upgrade/upgrade/IXP_bulkconfig_template /root/bulkconfig
```

Change the permission on the bulkconfig

```
# chmod 644 /root/bulkconfig
```

Unmount the MEDIATION iso file. As root run :

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

bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword, and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_gateway
ntpserver1,IP_address
ntpserver2,IP_address
ntpserver3,IP_address
ntppeerA,
ntppeerB,
nspprimary,IP_address_of_primary_weblogic_or_onebox_nsp_backend
nspsecondary,IP_address_of_secondary_weblogic
nsporacle,IP_address_of_oracle_server
timezone,time_zone
```

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

host Description

```
host,hostname_of_server,IP_address,function,interface_name,network_mask,network_gateway
```

...

Example (installation):

```
host,ixp1981-1a,10.236.2.141,IXP-XDR,eth01,255.255.255.224,10.236.2.129
```

There is one single host line per DWS.

Example of disaster recovery:

```
host,ixp1981-1a,10.236.2.141,DR-XDR,eth01,255.255.255.224,10.236.2.129
```

There is one single host line per DWS.

The host keyword has the following associated values:

PIC 10.1.5 Installation Guide

hostname_of_server The server hostname in the standard IXP format: ixpNNNN-MA where:

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

IP_address The IP address of the server. For blade systems, the backend (VLAN 3) IP address of the server.

function The function of the server. For installation:

- IXP-XDR

For disaster recovery:

- DR-XDR

interface_name Name of the interface where the network settings are applied.

- eth01 for the rackmount systems
- bond0.3 for the blade systems

network_mask The network mask.

network_gateway The default gateway.

ntpserver Description

Refer to Appendix 17 to know how to configure NTP.

```
ntpserver1,IP_address
ntpserver2,IP_address
ntpserver3,IP_address
ntppeerA,
ntppeerB,
```

- ntpserver1 is the first NTP server
- ntpserver2 is the second NTP server
- ntpserver3 is the third NTP server
- ntppeerA not applicable; leave empty
- ntppeerB not applicable; leave empty

Example:

```
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
```

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server.

NSP Description

```
nspprimary,IP_address_of_primary_weblogic_or_onebox_nsp_backend
nspsecondary,IP_address_of_secondary_weblogic
nsporacle,IP_address_of_oracle_server
nspadmin,IP_address_of_weblogic_admin_server
```

- nspprimary is the Management Server Primary WebLogic server or the One-box Management Server
- nspsecondary is the Management Server Secondary WebLogic server
- nsporacle is the Management Server Oracle server

- nspadmin is the Management Server Weblogic admin server

Note: The nspadmin entry is only needed when the Management server is installed on ODA. In case of ODA, nspprimary server shall depict weblogic managed server1 and nssecondary server shall depict weblogic managed server2

Example (for a One-box Management Server):

```
nspprimary,10.10.10.10
nssecondary,
nsporacle,
```

The NSP keyword has the following associated values:

IP_address_of_primary_weblogic_or_onebox_nsp_backend The IP address of the MANAGEMENT SERVER server:

- One-box: backend IP address of the One-box Management Server

IP_address_of_secondary_weblogic The IP address of the Management Server:

- One-box: not applicable; leave empty

IP_address_of_oracle_server The IP address of the Management Server Oracle server:

- One-box: not applicable; leave empty

Example (For ODA based Management Server):

```
nspprimary,10.10.10.11
nssecondary,10.10.10.12
nsporacle,10.10.10.9
nspadmin,10.10.10.10
```

The NSP keyword has the following associated values:

IP_address_of_weblogic managed server1 on ODA

IP_address_of_weblogic managed server2 on ODA

IP_address_of_oracle_server on ODA

IP address of weblogic admin server on ODA

timezone Description

```
timezone,time_zone
```

Example:

```
timezone,Europe/Paris
```

The timezone keyword has the following associated value:

time_zone

The timezone string. For a list of available timezones that you can use, refer to the /usr/share/zoneinfo/zone.tab file TZ column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT--
#code coordinates TZ comments
AD +4230+00131 Europe/Andorra
```

PIC 10.1.5 Installation Guide

```
909-2122-001 Revision 1.11, February 02, 2012 DRAFT 210
PIC Bulkconfig File Description
AE +2518+05518 Asia/Dubai
AF +3431+06912 Asia/Kabul
AG +1703-06148 America/Antigua
CZ +5005+01426 Europe/Paris
---CUT---
```

bulkconfig file: installation example

A bulkconfig file needs to be created for the following DWS:

- Hostname: ixp1981_1a
- IP address: 10.236.2.141
- Network interface: eth01
- Network mask: 255.255.255.254
- Default gateway: 10.236.2.129
- NTP server IP address: 10.236.129.11
- Management Server One-box IP address: 10.10.10.10
- Server timezone: Europe/Paris

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@ixp1981-1a ~]# cat /root/bulkconfig
host,ixp1981-1a,10.236.2.141,IXP-XDR,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
timezone,Europe/Prague
```

11.4 Acquisition Server Bulkconfig File Description

This topic describes the syntax and use of the acquisition server bulkconfig file.

The acquisition server bulk configuration file contains the overall configuration information. The **bulkConf.pl** script uses this single file to configure the IMF subsystem or PMF accordingly.

The bulkconfig file is a text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The file is unique per subsystem and is present on each server in the subsystem.

DO NOT remove the acquisition server bulkconfig file from the server or subsystem.

This topic provides a description of each keyword and parameter used in the bulkconfig file (bulkconfig). It is important to read and understand the contents of this file.

Bulkconfig file location and rights

File name: bulkconfig
 File path: /root/bulkconfig

Mount the Acquisition Server iso file. As root run :
 # mount -o loop /var/TKLC/upgrade/iso_file.iso /mnt/upgrade

Copy the good bulkconfig file template:
 # cp /mnt/upgrade/upgrade/XMF_bulkconfig_template /root/bulkconfig

Change the permission on the bulkconfig
 # chmod 644 /root/bulkconfig

Unmount the Acquisition Server iso file. As root run :
 # umount /mnt/upgrade

Bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_1st_server,IP_address,function,interface_name,network_mask,network_gateway,designation
host,hostname_of_2nd_server,IP_address,function,interface_name,network_mask,network_gateway,designation
host,hostname_of_nth_server,IP_address,function,interface_name,network_mask,network_gateway,designation
ntpserver1,IP_address
ntpserver2,IP_address
ntpserver3,IP_address
ntppeerA,IP_address
ntppeerB,IP_address
nspprimary,IP_address_of_primary_nsp
nspsecondary,IP_address_of_secondary_nsp
nspadmin,IP_address_of_welogic_admin_server_ODA
```

timezone,time_zoneRefer to the following descriptions of each keyword and its associated values. **host**

Description

```
host,hostname_of_1st_server,IP_address,function,interface_name,network_mask,network_gateway,designation
host,hostname_of_2nd_server,IP_address,function,interface_name,network_mask,network_gateway,designation
host,hostname_of_nth_server,IP_address,function,interface_name,network_mask,network_gateway,designation...
```

Example for IMF setup:

```
host,imf-1a,192.168.253.5,IMF,bond0.200,255.255.255.224,192.168.253.1,1A
host,imf-1b,192.168.253.6,IMF,bond0.200,255.255.255.224,192.168.253.1,1B
host,imf-1c,192.168.253.7,IMF,bond0.200,255.255.255.224,192.168.253.1,1C
```

Example for PMF standalone:

```
host,pmf-0a,192.168.2.106,PMF,eth01,255.255.255.0,192.168.2.1,0A
```

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

The host keyword has the following associated values:

hostname_of_nth_server The server hostname.

PIC 10.1.5 Installation Guide

Note: It is recommended that the hostname ends with the designation of the server (for example, malibu-1a).

function	The function of the server. Use one of the following entries: •he function
designation	The designation of the server is a combination of frame number and position of the server in the frame. Use the following rule: • IMF subsystem: 1A for the first server, 1B for the second server, etc. • F subsystem: 1A for
interface name	The name of customer network interface (typically: bond0.200 for IMF and eth01 for PMF)
IP_address	The IP address of the server. For blade systems, the internal IP address of the server
network_mask	The network mask
network_gateway	The default gateway

PIC 10.1.5 Installation Guide

IP_address_of_admin_server_nsp The IP address of the management admin server

timezone Description

timezone,time_zone

Example:

```
timezone,Europe/Paris
```

The timezone keyword has the following associated value:

time_zone The timezone string. For a list of available timezones that you can use, refer to the `/usr/share/zoneinfo/zone.tab` file **TZ** column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT--
#code      coordinates      TZ              comments
AD         +4230+00131      Europe/Andorra
AE         +2518+05518      Asia/Dubai
AF         +3431+06912      Asia/Kabul
AG         +1703-06148      America/Antigua
CZ         +5005+01426      Europe/Prague
---CUT---
```

Bulkconfig file: example

A bulkconfig file needs to be created for the following acquisition server subsystem:

- Subsystem hostname: imf-1a
- 1a server with the IP address: 192.168.253.5
- 1b server with the IP address: 192.168.253.6
- 1c server with the IP address: 191.168.253.7
- IMF subsystem, interface: bond0.200
- Network mask: 255.255.255.224
- Default gateway: 192.168.253.1
- NTP server IP address: 10.250.32.10
- Subsystem is added to the appserver with IP address: 10.10.10.10
- Subsystem timezone: Europe/Paris

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@T3-1A upgrade]# cat /root/bulkconfig
host,imf-1a,192.168.253.5,IMF,bond0.200,255.255.255.224,192.168.253.1,1A
host,imf-1b,192.168.253.6,IMF,bond0.200,255.255.255.224,192.168.253.1,1B
host,imf-1c,192.168.253.7,IMF,bond0.200,255.255.255.224,192.168.253.1,1C
ntpserver1,10.250.32.10
ntpserver2,10.250.32.11
ntpserver3,10.250.32.12
ntppeerA,10.250.32.13
ntppeerB,10.250.32.14
nspprimary,10.10.10.10
nspsecondary,10.10.10.11
nspadmin,10.31.3.82
timezone,Europe/Paris
```


12 APPENDIX: SWITCHES CONFIGURATION

Refer to E64544 PIC 10.1.5 Hardware Installation Guidelines

13 **APPENDIX: CAPACITY MANAGEMENT PROTRAQ CONFIGURATIONS**

PIC 10.1.5 Installation Guide

Pic_UsageStat_Mn.fse

```
SECTION:MAIN
# ProTraq
# Copyright (c) 2003, 2014, Oracle and/or its affiliates. All rights reserved.
# PIC_UsageStat_Mn, generated Tue Aug 05 08:07:48 EDT 2014
# PIC input bandwidth per server and per minute v1.0
VERSION:600
DLL:FSEQOS
MODE:AFTER
DESTINATION::PIC_UsageStats_Mn
ALARMPERIOD:60
ALARMSEVER::0
STATPERIOD:60:1814400
COMMENT:PIC input bandwidth per server and per minute v1.0
POINTCODEFORMAT:0:0:8:8:8:0
INSTANCE:
INSTANCEOID:

SECTION:CORNER:QUERY
NAME:PDU
EXPR:A
COND:A:Unit:=:1

SECTION:COLUMN:0:FIELD:Hostname of server (if applicable)
NAME:Server
STRING:Hostname:Hostname:Hostname:Host name of the server processing this flow.
  SIZE:128:DATA:MANDATORY::128
  ORACLE:VARCHAR2

SECTION:COLUMN:1:CUMULATIVE:Average Mbps per server to be compared to license RTU per server
NAME:LicensedMbps
FIELD:KbpsTotal
SCALE:1000
FILTER:0

SECTION:LINE:0:TOP:30:0:2
NAME:perServer
CRITERIA:Hostname:999:9999
ORDER:1:0
FILTER:1
EXPR:( C AND F AND G ) OR D
COND:C:CollectionPoint:=:ETH
COND:D:CollectionPoint:=:XBFINAL
COND:F:Direction:=:1
COND:G:DataFlow:<>:eth0*

SECTION:LINE:1:QUERY:30:0:6:EXCLUSIVE
NAME:Mediation Protocol 2
EXPR:( A OR B ) AND C AND ( E OR F OR G OR H OR I OR J OR K OR L )
COND:A:Role:=:4
COND:B:Role:=:5
COND:C:CollectionPoint:=:XBFINAL
COND:E:DataFlow:=:*LTE--DIAMETER-GY-rec
COND:F:DataFlow:=:*LTE--DIAMETER-S9-rec
COND:G:DataFlow:=:*LTE--RAN-EMM-reconst
COND:H:DataFlow:=:*LTE--GTP-v2-Mobility
COND:I:DataFlow:=:*LTE--RAN-ESM-reconst
COND:J:DataFlow:=:*RAN--CC2
COND:K:DataFlow:=:*SS7--SIGTRAN-TRANSP
COND:L:DataFlow:=:*SS7--EISUP-reconstit

SECTION:LINE:2:QUERY:30:0:7:EXCLUSIVE
NAME:Mediation Protocol
EXPR:( A OR B ) AND C
COND:A:Role:=:4
COND:B:Role:=:5
COND:C:CollectionPoint:=:XBFINAL

SECTION:LINE:3:QUERY:30:0:4:EXCLUSIVE
NAME:Probed Acquisition
EXPR:A AND B AND C AND D
```

```
COND:A:Role:=:2
COND:B:CollectionPoint:=:ETH
COND:C:Direction:=:1
COND:D:DataFlow:<>:eth0*

SECTION:LINE:4:QUERY:30:0:5:EXCLUSIVE
NAME:Integrated Acquisition
EXPR:A AND B AND C
COND:A:Role:=:1
COND:B:CollectionPoint:=:LINK
COND:C:Direction:=:1
```

PIC 10.1.5 Installation Guide

PIC_UsageStat.fse

```
SECTION:MAIN
# ProTraq
# Copyright (c) 2003, 2014, Oracle and/or its affiliates. All rights reserved.
# PIC_UsageStat, generated Tue Aug 05 05:49:21 EDT 2014
# Licensed Mbps average, min and max over 1 hour v1.0
VERSION:600
DLL:FSEQOS
MODE:AFTER
DESTINATION::PIC_UsageStats
ALARMPERIOD:1800
ALARMSEVER::0
STATPERIOD:3600:6048000
COMMENT:Licensed Mbps average, min and max over 1 hour v1.0
POINTCODEFORMAT:0:0:8:8:0
INSTANCE:
INSTANCEOID:

SECTION:COLUMN:0:FIELD:Hostname
NAME:Server
STRING:Server:Server:Server:Hostname of server (if applicable)
  SIZE:128:DATA:MANDATORY::128
  ORACLE:VARCHAR2

SECTION:COLUMN:1:CUMULATIVE:Average throughput
NAME:LicensedMbps
FIELD:LicensedMbps
SCALE:30
FILTER:0

SECTION:COLUMN:2:CUMULATIVE:Highest average in a minute
NAME:MaxMbps
FIELD:LicensedMbps
SCALE:1
RESULT:MAX
FILTER:0

SECTION:COLUMN:3:CUMULATIVE:Lowest average over one minute
NAME:MinMbps
FIELD:LicensedMbps
SCALE:1
RESULT:MIN
FILTER:0

SECTION:LINE:0:TOP:30:0:1:EXCLUSIVE
NAME:perServer
CRITERIA:Server:200:200
ORDER:1:0
FILTER:1
EXPR:A
COND:A:Line:=:perServer*

SECTION:LINE:1:QUERY:30:0:5:EXCLUSIVE
NAME:Mediation Protocol 2
EXPR:A
COND:A:Line:=:Mediation Protocol 2

SECTION:LINE:2:QUERY:30:0:6:EXCLUSIVE
NAME:Mediation Protocol
EXPR:A
COND:A:Line:=:Mediation Protocol

SECTION:LINE:3:QUERY:30:0:3:EXCLUSIVE
NAME:Probed Acquisition
EXPR:A
COND:A:Line:=:Probed Acquisition

SECTION:LINE:4:QUERY:30:0:4:EXCLUSIVE
NAME:Integrated Acquisition
EXPR:A
COND:A:Line:=:Integrated Acquisition
```

14 APPENDIX: HOW TO CONFIGURE NTP

The goal of this MOP is to reach the targeted NTP precision on the DS Wiki
http://cqweb/wiki/index.php/How_to_check_the_NTP_synchronization

- **Delay:** *Should be below 10 ms.*
- **Offset:** *Should be below 1 ms.*

14.1 NTP architecture

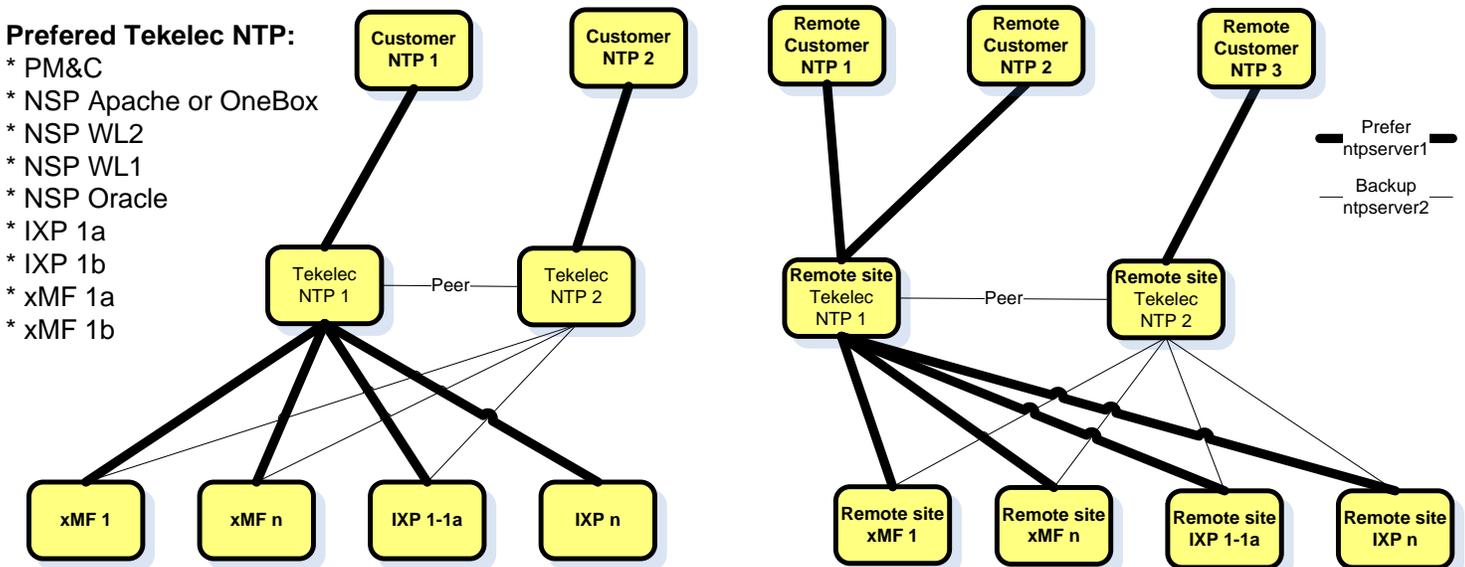
Configure two Tekelec servers as Tekelec NTP taking in account the preference described below.

On these servers NTP configure one or more customer NTP and the second Tekelec NTP as a peer. (see platcfg screenshot below). Make sure each Tekelec NTP are connected to “independent” NTP and don’t share the customer NTP servers.

On all other servers use these Tekelec NTP as ntpserver1 and ntpserver2. (see platcfg screenshot below)

Don’t configure the customer NTP as backup of the Tekelec NTP you selected!

If there are remote site(s) with poor NTP synchronization use some local servers as Tekelec NTP. This is especially the case when you have acquisition server or IXP installed on site in different regions from a big country and using a single Management Server.



14.2 Check the NTP precision

Wait sometime after the configuration and check the NTP using the command `ntpq -p` on each server

```
[cfguser@ixp0051-1z ~]$ ntpq -p
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*ntpserver1	10.16.0.2	3	u	1	16	377	0.180	1.013	0.023
+ntpserver2	192.5.41.41	2	u	1	16	377	0.292	9.233	0.044
+ntpserver3	192.5.41.41	2	u	2	16	377	0.264	1.108	0.064

15 APPENDIX: NETWORK PORTS BETWEEN PIC COMPONENTS

Refer to E56969 PIC 10.1.5 Security guide

16 APPENDIX: 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.

17 APPENDIX: 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. Under Industries, click the link for Oracle Communications documentation. The Oracle Communications Documentation window opens with Tekelec shown near the top.
2. Click Oracle Communications Documentation for Tekelec Products.
3. Navigate to your Product and then the Release Number, and click the View link (the Download link will retrieve the entire documentation set).
4. To download a file to your location, right-click the PDF link and select Save Target As.

18 APPENDIX: HOW TO ACCESS CONSOLE OF VM IN ODA

1. Login on ODA_BASE as root user with default password
2. Execute following command to get the VM names

```
$ oakcli show vm
```

3. Execute following command to access the VM console

```
$ oakcli show vmconsole <vm_name>
```

Name is obtained from step 2.