Oracle® Communications Performance Intelligence Center

OCPIC 10.4.0 Maintenance Guide

Release 10.4.0

F26312-03

March 2022

Oracle® Communications Performance Intelligence Center OCPIC 10.4.0 Maintenance Guide, Release 10.4.0

⚠ CAUTION: Use only the guide downloaded from Oracle Help Center (OHC).

Refer to Appendix section for instructions on accessing My Oracle Support and Oracle Help Center.

Table of Contents

MY ORACLE SUPPORT

My Oracle Support (MOS) is your initial point of contact for any of the following requirements:

- **Product Support:**

  The generic product related information and resolution of product related queries.

- **Critical Situations:**

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

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

Training Need:

Oracle University offers training for service providers and enterprises.

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.

1. INTRODUCTION

Overview

This document describes the procedures to maintenance "Oracle Communications Performance Intelligence Center" system at Release 10.4.0. This document covers disaster recovery procedures, IP change procedures as well as various application specific procedures.

This document is intended for use by trained engineers in software upgrade. A working-level understanding of oracle database, Linux and command line interface is expected to successfully use this document.

It is strongly recommended that prior to performing any operations, the user read through this document.

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

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

Requirements and Prerequisites

Hardware Requirements

Refer Hardware Guidelines of Performance Intelligence Center

Software Requirements

The following software is required for the Performance Intelligence Center 10.4.0.

Oracle Communication GBU deliverables:

- Management Server
- Mediation Server
- Mediation Protocol
- Acquisition Server
- TADAPT
- TPD
- TVOE
- PM&C
- Oracle Linux 7 for x86_64 bit

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

https://edelivery.oracle.com/

Please refer to KM notes:

Title	MOS
MOS **Oracle Database Appliance** - 12.1.2 and 2.X Supported ODA Versions & Known Issues (Doc ID 888888.1)	KM_888888.1
ZFS refer to MOS Oracle Support Document 2021771.1 (Oracle ZFS Storage Appliance: Software Updates)	KM_2021771.1

Note: In case of Disaster Recovery for DRS server installed before PIC 10.2, the release of PIC 10.1 must be considered.

Reference Documents

[1] 10.1.0 Installation Guide, E53508, Performance Intelligent Center release 10.1.0

[2] Installation Guide, F26308-01, Performance Intelligent Center release 10.4.0

[3] Upgrade document, F26309-01, Performance Intelligent Center release 10.4.0

[4] Quick Start Guide, F26315-01, Performance Intelligent Center release 10.4.0

[5] Hardware Guide, F26306-01, Performance Intelligent Center release 10.4.0

[6] PM&C Disaster Recovery, E54388-02 Release 5.7 and 6.0, November 2014

[7] Platform 7.0 Configuration Procedure References, E53486, December 2014

[8] TPD Initial Product Manufacturing, Tekelec Platform release 7.6

[9] OTD Administration Guide, E23389_01

[10] ODA Getting Started Guide, E22692-41, February 2015

[11] Teklec Default Passwords, CGBU_ENG_24_2229 (restricted access, refer to Appendix A: My Oracle Support)

[12] ZFS Storage Appliance Installation Guide, E55847-01, December 2014

[13] ZFS Storage Appliance Administration Guide, E55851-01, December 2014

[14] ZFS Administration Guide, E19253-01

2. Disaster Recovery Procedures on ODA/ZFS

DR of single or multiple Data Record Storage Server

ODA Physical Server Disaster

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

⚠ **Warning**: **Data from this Data Record Storage are lost because of the hardware failure and re-installation**

1. Set the Data Record Storage Server in maintenance mode by using Set Behavior Mode for Data Record Storage Server
2. Refer to **Chapter SYSTEM CONFIGURATION ON ODA of Installation document PIC 10.2.0 Installation document**
   a. Perform steps in section **OS installation,**
   b. Perform steps in section **ODA_BASE Template deployment**
   c. Perform steps in section **Creation of DRS database with ODA_BASE configurator**
   d. Perform steps in section **MEDIATION user and table spaces creation.**

   Note: If the ODA was hosting multiple Data Record Storage Server database, then step c) and d) should be repeated for the entire database.

3. Refer to Chapter **MEDIATION APPLICATION INSTALLATION PROCEDURES** of **Installation document PIC 10.2.0 Installation document**
   a. Perform steps in section **Mediation Server Pre-Install Configuration,**
   b. Perform steps in section **Install Mediation Server**
4. If the Data Record Storage Server was **active** before the DR**,** reset it to active mode using Set Behavior Mode for Data Record Storage Server

ODA_BASE Disaster

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

⚠ **Warning**: **Data will be lost.**

1. Set the Data Record Storage Server in maintenance mode by using Set Behavior Mode for Data Record Storage Server
2. Refer to **Chapter SYSTEM CONFIGURATION ON ODA of Installation document PIC 10.2.0 Installation document**
   a. Perform steps in section **OS installation,**
   b. Perform steps in section **ODA_BASE Template deployment**
   c. Perform steps in section **Creation of DRS database with ODA_BASE configurator**
   d. Perform steps in section **MEDIATION user and table spaces creation.**

Note: If the ODA was hosting multiple Data Record Storage Server database, then step c) and d) should be repeated for the entire database.

3. Refer to Chapter **MEDIATION APPLICATION INSTALLATION PROCEDURES** of **Installation document** PIC 10.2.0 Installation document
   a. Perform steps in section **Mediation Server Pre-Install Configuration,**
   b. Perform steps in section **Install Mediation Server**
4. If the Data Record Storage Server was **active** before the DR**,** reset it to active mode using Set Behavior Mode for Data Record Storage Server

Data Record Storage Server database re-creation

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

Note: This procedure normally should not affect the other Data Record Storage Server databases if present on the same ODA.

1. Set the Data Record Storage Server in maintenance mode by using Set Behavior Mode for Data Record Storage Server
2. Drop the database by using following steps.
   Database should be up before deleting.

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

```
# oakcli show databases

# oakcli delete database   -db <db_name>

# oakcli delete dbhome -oh <oracle_home>
```

   Where <db_name> is the Data Record Storage Server database name and <oracle_home> is oracle home for Data Record Storage Server database.

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

3. Refer to **Chapter SYSTEM CONFIGURATION ON ODA of Installation document** PIC 10.2.0 Installation document
   a. Perform steps in section **Creation of DRS database with ODA_BASE configurator**
   b. Perform steps in section **MEDIATION user and table spaces creation**

4. Refer to Chapter **MEDIATION APPLICATION INSTALLATION PROCEDURES** of **Installation document** PIC 10.2.0 Installation document
   a. Perform steps in section **Mediation Server Pre-Install Configuration**
   b. Perform steps in section **Install Mediation Server**
5. If the Data Record Storage Server was **active** before the DR**,** reset it to active mode using Set Behavior Mode for Data Record Storage Server

Note: IxpStore process on the mediation server should be restarted, after the above procedures are completed.

DR of ZFS

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

- ZFS storage appliance administration guide
- Chapter 11 in ZFS administration guide, http://docs.oracle.com/cd/E19253-01/819-5461/

1. **Disconnect the PDU directories shared by the ZFS**

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

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

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

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

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

   ```
   # bc_adjust_subsystem.sh
   ```

2. **DR the ZFS**

   Refer documents **ZFS storage appliance administration guide**

3. **Reconnect the PDU directories shared by the ZFS**

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

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

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

   ```
   # bc_adjust_subsystem.sh
   ```

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

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

3. Management Server Disaster Recovery Procedures

Management Server

This procedure describes the disaster recovery procedure of the Management Server. This procedure is a high-level procedure and some of the complex parts are referenced from different procedures.

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

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

Note:

1. The latest global backup must be copied to the external server before starting the DR. Copy the backup from external server to the management server box at "/opt/oracle/backup/", before the nsp application installation i.e. before executing "install_nsp.sh". We recommend verifying the backup content. As explained in the "Check Management Server Backup is valid" of the document 10.4 Upgrade Guide. Refer to Chapter 8 in 10.4 Installation Guide or Chapter 9 in 10.4 Upgrade Guide for Disaster Recovery on the OL and TPD based system respectively.

- During execution of "install_nsp.sh", user will be prompted to enter the NSP database password. In case database password is never changed, provide the default password else provide the latest NSP database password.

1. Install Management Server using Management Server (NSP) on Third-Party Server -Chapter 8 in 10.4.0 Installation Guide or Chapter 9 on TPD based platform in 10.4.0 Installation Guide
2. Check permission for backup directory
   Execute following commands as root:

   ```
   # cd /opt/oracle/backup

   # chmod a+w nsp_backup_timestamp

   # chown root:root nsp_backup_timestamp
   ```

   Where nsp_backup_timestamp refers to the backup directories created nightly

   Note: Management Server creates two different types of backups

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

3. **Restore the database and realm**

Following the steps:

a. Restore Realm Backup
b. Recover MGMT Database

4. **Reboot the server**

5. **Log in on the server and Run the install script for builders**
   As root, run:

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

# ./install_builder.sh
```

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

6. **Set Global Names to false**

```
# su - oracle

# sqlplus / as sysdba

# ALTER SYSTEM SET GLOBAL_NAMES=FALSE;
```

7. **Perform NSP Post-Install Sanity Check**
   Follow the step **NSP Post-Install Sanity Check**

If Management Server did not install successfully, refer to **My Oracle Support** with the NSP log files defined in the SRDC – How to Collect NSP logs section in Chapter 7: Management Server Maintenance Procedures You can extract them also with the following script:

```
#tarNSP
```

Restore Realm Backup

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

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

1. Log in as `root` on Management Server all following commands are executed as root
2. Execute the following commands:
   Note: Make sure the backup is from the same Management Server release which needs to be imported. You can check the release in the NSP_BACKUP_xxxx by opening it in a wordpad and read the iso_version of global_versions.porperties.

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

```
# cd /opt/nsp/scripts

# ./LaunchImpNSPrealm.sh backup_dir
```

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

Recover Database

Recover Management Server Database

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

1. Prerequisites for using Import Utility to Restore a Database

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

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

- Prerequisite for restoring a database

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

  Note: Check the ownership of the directory "/opt/oracle/backup". If the ownership is not oracle: oinstall, perform the below step:

  As root user

  ```
  # chown oracle:oinstall /opt/oracle/backup
  ```

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

  Otherwise, use the following command to set write permission:

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

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

  as root user go to folder <DIR_CONTAINING_DUMP>:

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

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

2. Import utility

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

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

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

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

a) Log in as `root` on Management Server and launch the command:

```
# service nspservice stop
```

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

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

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

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

The script has four parameters:

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

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

d) Log in as `root` on Management Server and launch the command:

```
# service nspservice start
```

Recover the wallet and oracle DB connections

Use the same daily backup directory, as for Realm and Database restoration

1. As tekelec user replace existing ewallet.p12 and cwallet.sso

```
# cd /u01/app/oracle/product/12.1.0/dbhome_1/wallet

# cp /usr/TKLC/nsp/<BACKUP_DIR>/wallet/cwalet.sso cwallet.sso

# cp /usr/TKLC/nsp/<BACKUP_DIR>/wallet/ewallet.p12 ewallet.p12

# chown oracle: oinstall ewallet.p12

# chown oracle: oinstall cwallet.sso
```

2. As root user replace existing tnsnames.ora and sqlnet.ora located

```
# cd /u01/app/oracle/product/12.1.0/dbhome_1/network/admin

# cp /usr/TKLC/nsp/<BACKUP_DIR>/wallet/network/admin/sqlnet.ora sqlnet.ora

# cp /usr/TKLC/nsp/<BACKUP_DIR>/wallet/network/admin/tnsnames.ora tnsnames.ora

# chown oracle: oinstall sqlnet.ora

# chown oracle: oinstall tnsnames.ora
```

3. As tekelec user Update credentials in IXP-Base and xMF servers (optional step):

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

# sh syncFiles.sh
```

Management Server Post-Install Sanity Check

1. Open a terminal window and log in as root on the Management Server
2. As root, run:

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

3. Review the Management Server installation logs (/var/log/nsp/install/nsp_install.log).
4. Verify the following:
   - PORT 80 is DISABLED

- Oracle server health is OK
- WebLogic health for ports 5556, 7001, 8001 is OK
- Log on to weblogic console and Verify the following**:**
  - All servers are in running and in OK state
  - Application deployments are in Active and OK state.

4. Acquisition Disaster Recovery Procedures

Acquisition Server Disaster Recovery

Reinstall Operating System

In case of real hardware the server must be IPM with TPD using steps mentioned below

Refer to PIC 10.4.0 Installation document for IPM instructions.

Or

In case of virtual machines, the Operating system must be re-installed using following procedure:

Section **"Guest OS Re-installation"** from PIC 10.4.0 Installation document

Install Acquisition Application

Refer to PIC 10.4.0 Upgrade document

5. Mediation/ Data Record Storage Server Disaster Recovery Procedures

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

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

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

Mediation/ Data Record Storage Server Disaster Recovery Overview

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

The procedure is applicable to the following server types:

- Data Record Storage Server
- PDU Storage Server
- Mediation Base Server

The procedure is applicable to the following hardware types:

- HP Gen8 Rackmount
- HP Gen9 RackMount
- ODA

Note: In case of DR performed on the DRS and PDU server based on TPD platform, the xDRs and PDUs stored already shall be preserved.

Data Record Storage disaster recovery procedure

Check the Oracle version on the Data Record Storage Server as root with the following command:

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

If Oracle 10g is installed, the disaster recovery procedure can not be applied and you have to go for a new installation (refer to PIC 10.4.0 Installation document, section of flow chart for DRS server) and the data are not preserved.

During the disaster recovery procedure of Data Record Storage Server, applicable to 11g or 12c, you must install the same version of the Oracle database as the current one.

If Oracle 11g is currently installed then the PIC 10.1 software release for DRS must be used.

Standard server Data Record Storage Server disaster recovery procedure

Follow the references below in a sequential order to recover the Data Record Storage server.

1. **Set the Data Record Storage server in** maintenance mode, follow Set Behavior Mode for Data Record Storage Server
2. **Refer to the Chapter 6 for "Data Record Storage Server" mentioned in PIC 10.4.0 Installation Guide**

3. **If the** Data Record Storage Server **was active before the DR, reset it in active mode using** Set Behavior Mode for Data Record Storage Server

ODA Data Record Storage Server disaster recovery procedure

Refer Chapter 2.1

HP or X6-2L Data Record Storage Server disaster recovery procedure

Follow the references below in a sequential order to recover the Data Record Storage server.

1. **Set the Data Record Storage server in** maintenance mode, follow Set Behavior Mode for Data Record Storage Server
2. **Refer to** **PIC 10.4.0 Installation document**, **Chapter 6 DWS Installation Procedures**
   Note:
   - Bulkconfig file must contain DR-XDR platform function value.
   - Execute all the other steps until Integration to customer network (this is the last step of the Data Record Storage Server Installation procedure to execute).
3. **If the** Data Record Storage Server **was active before the DR, reset it in active mode using** Set Behavior Mode for Data Record Storage Server

PDU Storage server disaster recovery procedure

Standard server PDU Storage Server disaster recovery procedure

In case the PDU storage server is based on **standard Oracle Linux** platform then DR shall involve the fresh installation using the Chapter 7 for "Packet Data Unit Storage Installation" mentioned in PIC 10.4.0 Installation Guide

Mediation PDU Storage server disaster recovery procedure

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

The PDU storage server is part of the mediation sub-system and supports base server processing.

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

1. **Stop IXP service using** Stop IXP Service (if the server is accessible)
2. **Disintegrate Server with Mediation Subsystem** Disintegrate Server with the Mediation Subsystem
3. **Refer to** **PIC 10.4.0 Installation document**, **Section "Mediation Subsystem" installation procedures.**
   Note:
   - Bulkconfig file must contain DR-PDU platform function value.
4. Integrate Server with in mediation sub-system using Integrate Server with the Mediation Subsystem
5. **Remount Export Directories using** Remount Export Directories

Mediation Base server disaster recovery procedure

Follow the references below in a sequential order to recover Mediation Base server: Mediation PDU Storage server disaster recovery procedure, with the following differences:

- **In the bulkconfig file, use DR-BASE as the platform function value (instead of DR-PDU).**
- **If the server is a virtual machine, follow the section "Mediation Guest OS reinstallation" from** PIC 10.4.0 Installation document **(instead of the section "Mediation Subsystem")**

Stop IXP Service

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

Open a terminal as root on the mediation server:

```
# service TKLCixp stop
```

Disintegrate Server with the Mediation Subsystem

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

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

   Analyze the output of the script for errors. Issues reported by this script must be resolved before any further usage of this server. Verify no errors are present (ignore error messages regarding the server that is going to be disintegrated for the subsystem).

   If errors occur, refer to **Appendix A: My Oracle Support**

2. **Remove a host record from the bulkconfig file**
   a) As root user, remove a host record with the server you want to disintegrate from the /root/bulkconfig file.
   b) Make sure, now the /root/bulkconfig file contains all remaining servers in the subsystem with valid parameters.
3. **Update mediation subsystem servers**
   a) Run the following script to adjust the mediation subsystem network and other settings accordingly to the /root/bulkconfig file. As root run:
   ```
   # /usr/TKLC/plat/sbin/rootSshLogin --permit

   # bc_adjust_subsystem.sh
   ```

   b) Wait until system reconfigures.
   c) Verify that the mediation subsystem has been reconfigured correctly. As root run:
   ```
   # bc_diag_bulkconfig.sh -a
   ```

   If any error occurs refer to **My Oracle Support**

Integrate Server with the Mediation Subsystem

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

1. **Add a host record to the bulkconfig file with the recovered server**
   a) Open a terminal window and log in to the recovered server as root user.
   b) Recreate the /root/bulkconfig file. You can copy the content of the /root/bulkconfig from

any other server in the mediation subsystem.

c) Add a host record for the recovered server with the valid information into the /root/bulkconfig file.

d) Make sure, now the /root/bulkconfig file contains all servers in the subsystem with valid parameters.

2. **Restore shared directories and Data Feed status**

a) Restore possible shared directories by running, as root:

```
# ixp_postinstall_restore.sh
```

b) Restore Data Feed status by running, as root:

```
# RestoreDataFeedStatus.sh --local
```

3. **Update Mediation subsystem**

Refer to **Update mediation subsystem servers.**

4. **Sync Database Credentials**

Execute procedure in section **Sync Database Credentials**

5. **Copy the xDR Builder rpm if not present**

a) Login into Management Server as root user and execute the below command to check if the xDR builder rpm is present.

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

If the above command shows, the xDR builder rpm then do not execute step b).

b) Copy the xDR builder rpm to path /var/TKLC/jmxagent/upload/

Note: xDR builder rpm, which is mentioned in load line up

6. **Install the xDR Builder package**

All servers in the Mediation subsystem must have the same xDR builders package.
As cfguser run:

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

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

Remount Export Directories

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

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

```
$ sudo umount /opt/TKLCdataexport/mount/*
```

3. **DataFeed will mount exporting directories back by itself.**

6. IP Changes Procedure

The Performance Intelligence Center IP change procedure are defined for the system, which are installed over **TPD** platform.

IP Change Overview

The IP change procedure is applicable to already configured system that is in running state.

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

Note: This procedure must be run via ILO

1. **Disable all feeds associated with Mediation subsystems**
   Note: Execute this step if you are going to migrate Mediation subsystem.

   a. Open a web browser, log in to Management Server application interface, and navigate to **DataFeed** application.
   b. Click on **xDR/KPI Feeds** and deactivate all feeds that are associated with the Mediation subsystems that going to be migrated to new network settings
2. **Management Server IP Change Procedure**
3. **Acquisition subsystem IP Change Procedure**
4. **Mediation Subsystem IP Change Procedure**
5. **Data Record Storage Server IP Change Procedure**
6. **Enable all feeds associated with Mediation subsystems**
   Note: Execute for all feeds that has been deactivated before IP change procedure.

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

Management IP Change Procedure

For Management Server, which is no more TPD based with 10.4.0, the IP change procedures is no more provided and has to be managed by the customer.

Acquisition subsystem IP Change Procedure

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

Note: This procedure must be run via ILO

Change IP Addresses

Run this procedure as root:

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

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

3. Reboot the server

Change VIP Addresses

Note: This is run on the primary server only

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

     ```
     setSSVIP -s
     ```

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

     ```
     setSSVIP <VIP>
     ```

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

Change IP Address Acquisition subsystem in Management

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

Mediation Subsystem IP Change Procedure

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

Use this procedure in following cases:

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

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

Note: This procedure must be run via ILO

1. **Update the bulkconfig file**

   a. Login to the iLO as root of any Mediation server in the subsystem you are about to reconfigure

   b. Update the /root/bulkconfig file with the new IP addresses

2. **Run IP change procedure**

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

   ```
   # bc_changeip_subsystem.sh
   ```

   b. The Mediation subsystem health check procedure will be triggered.

   c. If the health check procedure will end with no errors then the script will automatically continue with the IP change procedure. If there will be errors you will be asked for confirmation if you want to continue. In such case, **refer to** Appendix A: My Oracle Support before answering.

   d. If you migrate, the Mediation subsystem in a scope of a single network the script will run until the end and there is no additional operation needed.

   e. Perform any hardware related configuration like cabling etc.

   f. Log in to the server where you have previously updated the bulkconfig file as root and run:

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

   Wait until the procedure finishes. Check for any errors. In case of any errors, **refer to** My Oracle Support

Note: These steps mentioned in point three, four and five have to be performed on the management server

3. **Change Mediation subsystem IPs in Management**

   a. Login to the Management Server GUI and navigate to **Centralized Configuration** Application

   b. Navigate to **Equipment Registry** in Left Tree Panel

   c. Click on **IXP** ➤ **IXP Subsystem**

   d. Modify the servers and change **Admin IP address** field to the new IP address

4. **Change Mediation subsystem's VIP in Management Server**

   a. Login to the Management Server GUI and navigate to **Centralized Configuration** Application

   b. Navigate to **Equipment Registry** in Left Tree Panel

   c. Click on **Mediation**

   d. Modify the subsystem and change **VIP Address** field to the new IP address

   e. Click Modify

   f. **Execute Procedure Sync Database Credentials**

5. **Apply changes**

   a. Navigate to the **Mediation** view

   b. Navigate to **Sites**

   c. Open **IXP** and right-click on the subsystem.

   d. Select **Apply changes…** from the popup menu.

   e. Click on the **Next** button

f. Click on the **Apply Changes** button.

g. Wait until changes are applied.

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

Data Record Storage Server IP Change Procedure

This procedure describes how change the IP settings on the Data Record Storage Server.

This procedure is applicable **only for the TPD based** Data Record Storage server.

For ODA or Standard Server, the IP change procedures is not provided and has to be managed by the customer.

Use this procedure in following cases:

- Server IP change
- Netmask change
- Default gateway change

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

Note: This procedure must be run via ILO

1. **Update the bulkconfig file**

   a. Login to the iLO as root other Data Record Storage Server you are about to reconfigure

   b. Update the `/root/bulkconfig` file with the new IP addresses

2. **Run IP change procedure**

   a. Run the Data Record Storage Server subsystem IP change procedure as root:

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

   b. Continue with:

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

   c. Continue with:

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

   d. Finalize the IP change procedure on the Data Record Storage Server, as cfguser:

```
$ makeDWH.sh
```

   Confirm, enter passwords where needed.

   e. Reconfigure the dbconsole

   Log into the DRS server, as oracle user

```
# cd $ORACLE_HOME/bin
# ./emca -deconfig dbcontrol db -repos drop
```

This command prompts to provide following information as :

```
Database SID:

Listener port number:

Password for SYS user:

Password for SYSMAN user:
```

After providing this information, the system asks for confirmation as:

```
Do you wish to continue? [Yes(Y)/no (N)]:
```

After successful completion of command, it gives following message:

```
INFO: Repository successfully dropped
```

Enterprise Manager Configuration completed successfully

```
FINISHED EMCA at <DATE>

# ./emca -config dbcontrol db -repos create
```

This command prompts to provide some information.

Provide only the mandatory information and let it take the default value.

The command prompts to provide following information:

```
Database SID:

Listener port number:

Listener ORACLE_HOME [ /opt/oracle11/oracle/product/11.2.0/dbhome_1 ]:

Password for SYS user:

Password for DBSNMP user:

Password for SYSMAN user:

Email address for notifications (optional):

Outgoing Mail (SMTP) server for notifications (optional):

ASM ORACLE_HOME [ /opt/oracle11/oracle/product/11.2.0/dbhome_1 ]:

ASM SID [ +ASM ]:

ASM port [ 1521 ]:

ASM username [ ASMSNMP ]:

ASM user password:
```

After providing this information, the system asks for confirmation as:

```
Do you wish to continue? [Yes(Y)/no (N)]:
```

After successful completion of command, it gives following message:

```
Enterprise Manager Configuration completed successfully

FINISHED EMCA at <DATE>
```

Note: These steps mentioned in point three and four have to be performed on the management server

3. **Change Data Record Storage Server IP in Management Server**
   a. Login to the Management Server GUI and navigate to **Centralized Configuration** Application
   b. Navigate to **Equipment Registry** in Left Tree Panel
   c. Click on **DWS ➤ DWS Pool**
   d. Modify the Data Record Storage Server and change **Admin IP address** field to the new IP address
   e. Execute step of chapter 7 about **Modify Database Password** , with same password to create the tnsalias with new IP address.
4. **Apply changes**
   a. Navigate to the **Mediation** view
   b. Navigate to **Sites**
   c. Open **IXP** and right-click on the subsystem.
   d. Select **Apply changes…** from the popup menu.
   e. Click on the **Next** button
   f. Click on the **Apply Changes** button.
   g. Wait until changes are applied.
   h. Verify that result page does not contain any errors.

7. Management Server Maintenance Procedures

Management Server Backup Procedures

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

Automatic Backup

Activate Automatic Management Server Backup

This procedure describes how to activate the automatic backup procedure.

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

1. **Verify if the backup is activated**

   a. Login as `root` on Management Server - all following commands are executed as root

   b. Check the cron job list

   ```
   # crontab -l
   ```

   Example of output when backup is already activated:

   ```
   00 22 * * * . $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd; sh

   ./LaunchExpNSPdp.sh >../trc/cronNSP.log 2>&1
   ```

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

   Example of output when backup is not activated:

   ```
   no crontab for root
   ```

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

2. **Activate backup**

   Run the following commands as root:

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

   # crontab crontab.nsp
   ```

3. **Verify if the backup is activated and functional**

   a. Backup files are stored in the `/opt/oracle/backup/` directory on a daily basis on the Management Server. Each subdirectory contains a timestamp of the backup.

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

   b. For an Management Server, the directory structure is:

NSP_BACKUP_TIMESTAMP containing:

- A log file. It contains any information useful to troubleshoot a backup error.
- Database dump and log
- LDAP backup
- System files backup.

Deactivate Automatic Management Server Backup

This procedure describes how to deactivate automatic Management Server backup.

a. Login as root on Management - all following commands are executed as root
b. Check the cron job list

```
# crontab -l
```

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

c. Edit the contents of the crontab

```
# crontab -e
```

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

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

```
# crontab -l

00 22 * * * . $HOME/.bash_profile; cd        /opt/nsp/scripts/oracle/cmd; sh

./LaunchExpNSPdp.sh >../trc/cronNSP.log 2>&1
```

Change Automatic Management Server Backup Time and Location

Execute this procedure to change an automatic backup time or location

1. **Change Automatic Management Server Backup Time**

a. Login as `root` on Management Server - all following commands are executed as root
b. Check the cron job list

```
# crontab -l
```

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

c. Edit the contents of the crontab

```
# crontab -e
```

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

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

```
00 22 * * * . $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd; sh

./LaunchExpNSPdp.sh >../trc/cronNSP.log 2>&1
```

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

```
30 13 * * * . $HOME/.bash_profile; cd /opt/nsp/scripts/oracle/cmd; sh

./LaunchExpNSPdp.sh >../trc/cronNSP.log 2>&1
```

2. **Change Automatic Management Server Backup Location**

a. To change the location of where the backup files are stored runs the following command. As `root` run:

b. Edit the **LaunchExpNSPdp.sh** file using a text editor. Replace any occurrence of `/opt/oracle/backup` with a different backup directory.

c. Save changes.

Management Server Database Backup

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

1. Login as a `root` user on Management Server - all following commands are executed as root
2. Create a directory having write permission for the Oracle user:

```
# mkdir /opt/oracle/backup

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

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

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

# ./ExpNSPdp.sh NSP/NSP NSP /opt/oracle/backup
```

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

This script has three parameters and constraints:

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

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

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

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

# ./ExpNSPdpNoEXPT.sh NSP/NSP NSP /opt/oracle/backup
```

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

Realm Backup

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

1. Login as `root` user on Management Server
2. Execute following commands to take back up. As `root` run:

```
# cd /opt/nsp/scripts

# cp -u

/usr/TKLC/nsp/nsp-
package/framework/install/dist/install/post_installation/LaunchExpNSPrealm.sh

 /opt/nsp/scripts

# mkdir /opt/nsp/realmbackup

# ./LaunchExpNSPrealm.sh /opt/nsp/realmbackup
```

3. Verify the backup exist in /opt/nsp/realmbackup. Now backup this directory to an external media.

System Files Backup

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

1. Login as `root` user on Management Server
2. Execute following commands to take back up. As `root` run:

```
# cd /opt/nsp/scripts

# ./ExpNSPSys.sh backup_directory
```

Where *backup_directory* is any directory with write access for root user where the backup file will be created.

Copy Management Backup

1. **Copy Management Server Backup**

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

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

- It will ask for backup user password, enter the password for backup user and press ENTER.
- **nsp-ip** should be replaced by the Management server's IP address
- */path/to/backup/dir* should be replaced by exact path of backup on server. For example*/opt/backup/backup/NSP_BACKUP_09_13_11_22_00_01*
- To note exact path of the backup you can use steps mentioned in step 2 below.
- *local_backup_dir* should be replaced by a directory name of the Customer choosing.
- After successful completion of the command the backup should be available at the *local_backup_dir* folder.

  In case of any error contact MOS

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

a. Login as root on Management Server One-Box server

b. Note the path of the backup to be copied by executing the command below:

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

It should output something like:

```
drwxrwxrwx 5 root root 4096 Sep    7 22:25

/opt/backup/backup/NSP_BACKUP_09_07_11_22_00_01

drwxrwxrwx 5 root root 4096 Sep    8 22:26

/opt/backup/backup/NSP_BACKUP_09_08_11_22_00_01

drwxrwxrwx 5 root root 4096 Sep    9 22:25

/opt/backup/backup/NSP_BACKUP_09_09_11_22_00_01

drwxrwxrwx 5 root root 4096 Sep 10 22:25

/opt/backup/backup/NSP_BACKUP_09_10_11_22_00_02

drwxrwxrwx 5 root root 4096 Sep 11 22:26

/opt/backup/backup/NSP_BACKUP_09_11_11_22_00_01

drwxrwxrwx 5 root root 4096 Sep 12 22:28

/opt/backup/backup/NSP_BACKUP_09_12_11_22_00_01

drwxrwxrwx 5 root root 4096 Sep 13 22:26

/opt/backup/backup/NSP_BACKUP_09_13_11_22_00_01
```

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

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

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

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

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

It should output something like:

```
/opt/backup/backup/ALA_2011_07_01.csv

/opt/backup/backup/ALA_2011_07_12.csv

/opt/backup/backup/ALA_2011_07_23.csv

/opt/backup/backup/ALA_2011_07_02.csv

/opt/backup/backup/ALA_2011_07_13.csv

/opt/backup/backup/ALA_2011_07_24.csv

/opt/backup/backup/ALA_2011_07_03.csv

/opt/backup/backup/ALA_2011_07_14.csv

/opt/backup/backup/ALA_2011_07_25.csv
```

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

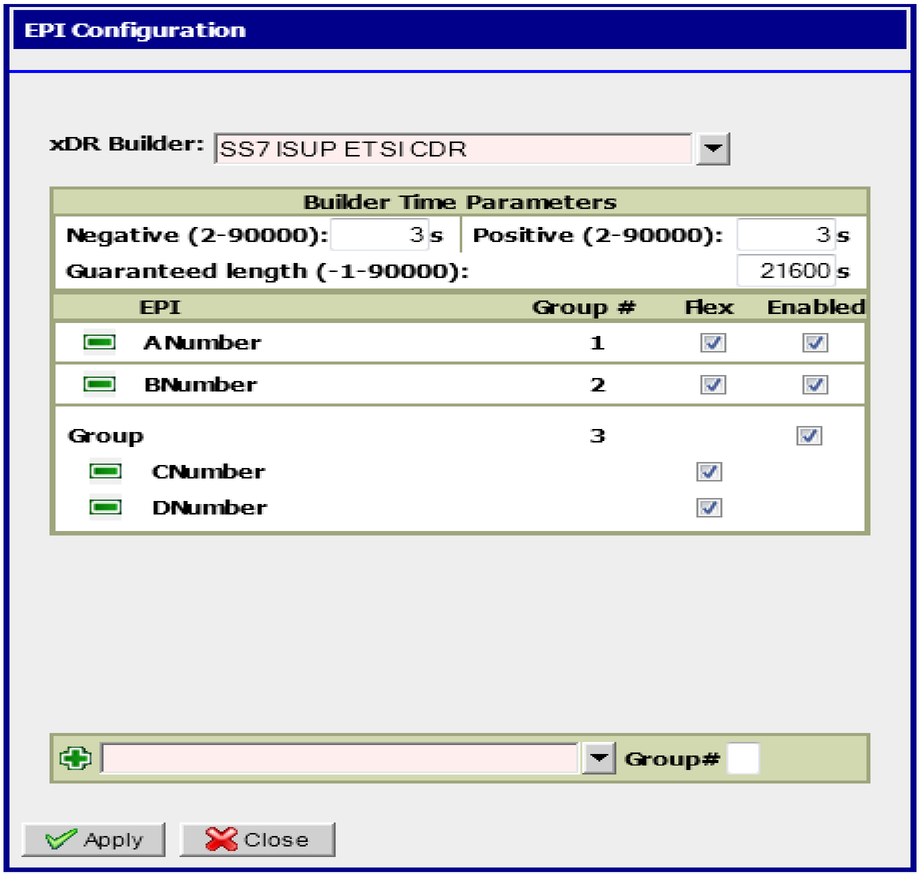
EPI and Plugin Configuration for Tracing

EPI Configuration

a) From Internet Explorer, connect to the Management Server Application GUI using the following URL: ***http://nsp_ip/nsp***
Where nsp_ip is the IP address of the Management Server
b) Login with user TklcSrv
c) Launch ProTrace Application from Applications

Configuring Builder Time Tolerance Parameters

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



EPI Configuration

xDR Builder: SS7 ISUP ETSI CDR

Builder Time Parameters

Negative (2-90000): 3 s Positive (2-90000): 3 s

Guaranteed length (-1-90000): 21600 s

EPI	Group #	Flex	Enabled
ANumber	1	☑	☑
BNumber	2	☑	☑
Group	3		☑
CNumber		☑	
DNumber		☑	

Group#

c) Fill in the Builder Time Parameters.
The Builder Time Parameters define the time range used for searching for new xDRs. This time range is related to BEGIN TIME and END TIME of discovered xDRs and uses a Positive and a Negative value.

The ranges for both positive and negative rules are 2-90000 seconds.

The Guaranteed length parameter allows you to enhance the search period to END_TIME + Guaranteed length. This parameter is used for search optimization and corresponds to the longest call or transaction the system is guaranteed to find.

d) Click on Apply to Save. The Builder Time Tolerance parameters would be saved successfully.

Add EPI

a) Open the EPI Configuration UI and Select a Builder. As in Section 9.8.1.1, a) and b)
b) Define the EPI's and EPI parameters for that builder.
EPI Name – Select any dictionary field from the drop down.

Group Number – Specify the group number in which you want to add EPI. If group number were blank, then the default Group Number during Add operation would be the Max Group Number + one (max for the selected builder

c) Click Add button. The EPI will be added in the list.
    - Flex and Enabled would be checked by default
d) Click Apply. The changes are saved.

Delete EPI

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

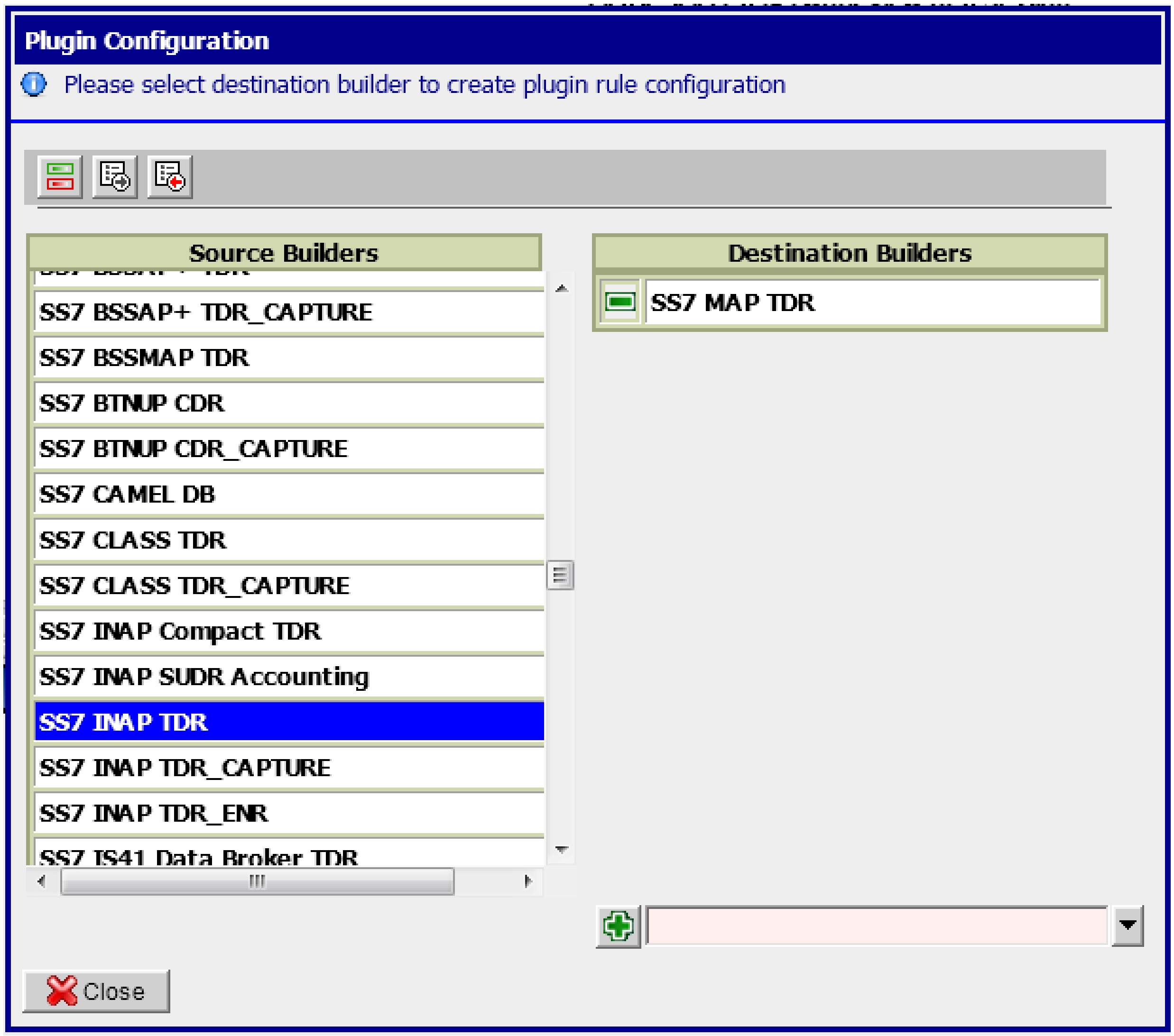
Update EPI

a) Open the EPI Configuration UI and Select a Builder. As in Section 9.8.1.1, a) and b)
b) Select (or de-select), the EPI parameters for that protocol.
    - Flex - defines whether the "Flex matching" is used for given field
c) Click Apply. The changes are saved.

Configuring Plugins

Create Plugin

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



Plugin Configuration

Please select destination builder to create plugin rule configuration

Source Builders
SS7 BSSAP+ TDR_CAPTURE
SS7 BSSMAP TDR
SS7 BTNUP CDR
SS7 BTNUP CDR_CAPTURE
SS7 CAMEL DB
SS7 CLASS TDR
SS7 CLASS TDR_CAPTURE
SS7 INAP Compact TDR
SS7 INAP SUDR Accounting
SS7 INAP TDR
SS7 INAP TDR_CAPTURE
SS7 INAP TDR_ENR
SS7 IS41 Data Broker TDR

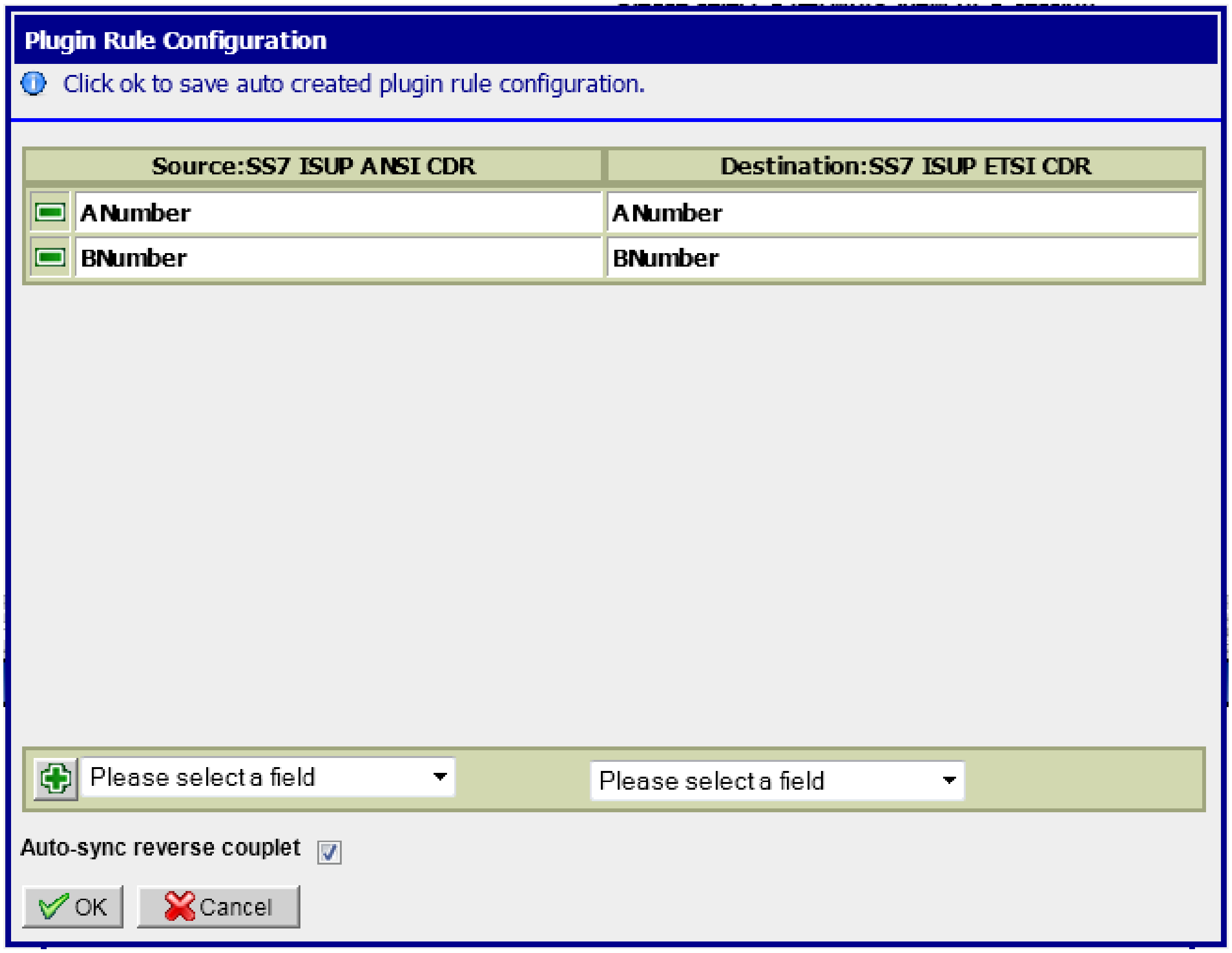
Destination Builders
SS7 MAP TDR

b) Click on Source Builder to configure. In the right pane all builders mapped with this source builder are populated.

c) To add a new plugin, select the destination builder from the available builders drop down

d) Click on Add Button

e) Plugin Rule Screen will open



Plugin Rule Configuration

Click ok to save auto created plugin rule configuration.

Source:SS7 ISUP ANSI CDR	Destination:SS7 ISUP ETSI CDR
ANumber	ANumber
BNumber	BNumber

f) Auto created Plugin Rules for the selected source and destination builders will be displayed. Auto Creation is done for the EPI's which are common to both the builders e.g. if ANumber is an EPI for both Source and Destination Builder a Plugin Rule ANumber → ANumber will be auto created in GUI.

g) If some auto created rules are not required, user can optionally delete them

h) If some more rules are required to be added user can optionally add more rules

i) The Auto-sync reverse couplet Check Box if checked would create a plugin in reverse direction as well when the Plugin is saved

j) Click on Add Button to create a Plugin Rule after selecting Source and Destination Fields

k) Click on Ok to Save the Configuration. Plugin would be created.

Update Plugin

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

b) Click on Source Builder to configure. In the right pane, all builders mapped with this source builder are populated.

c) Click on the Destination Builder to Edit Plugin

d) Plugin Rule Screen will be opened

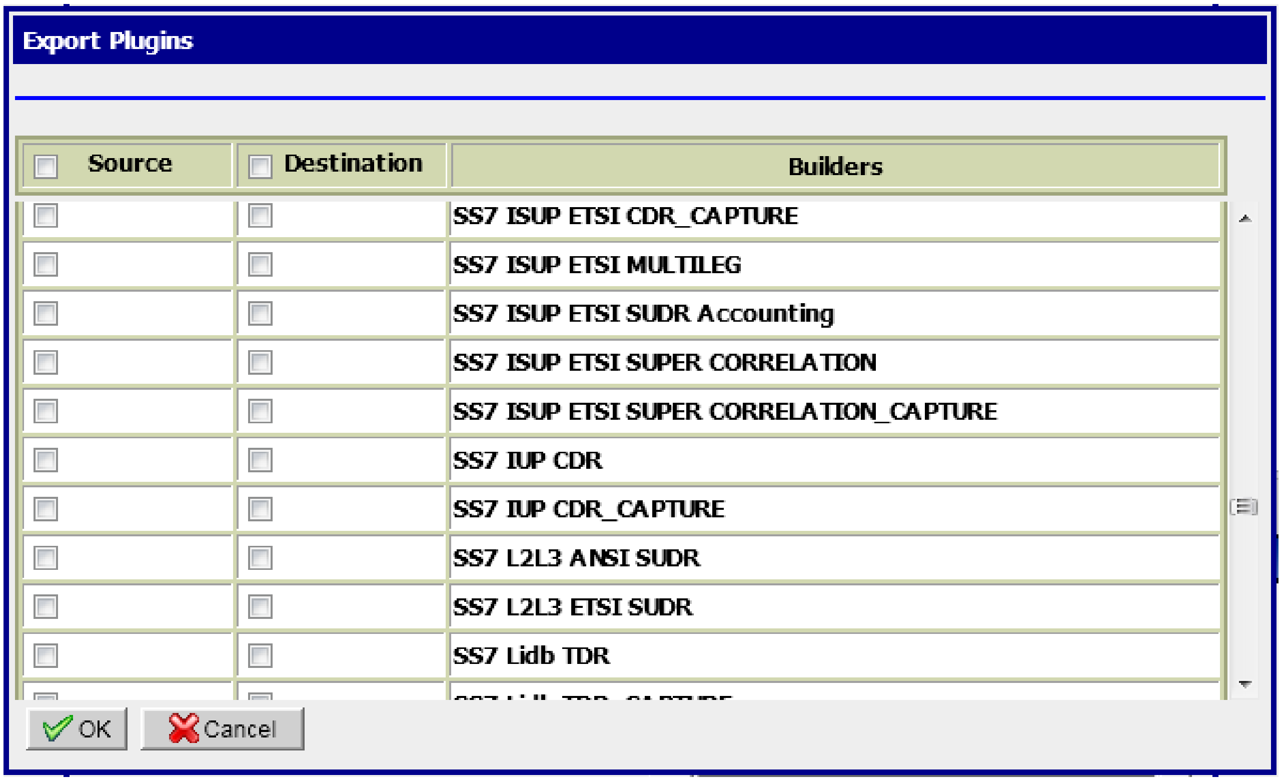
e) Add/Delete required Plugin Rules
f) Click on Ok Button.
g) Plugin would be updated with new rules

Delete Plugin

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

Export Plugin Configuration

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



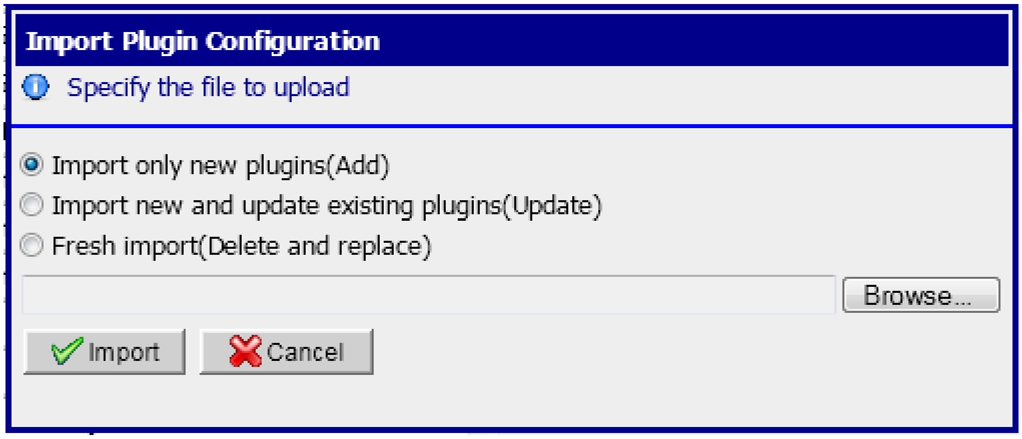
Export Plugins

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

Import Plugin Configuration

Using GUI

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



Import Plugin Configuration

Specify the file to upload

● Import only new plugins(Add)
○ Import new and update existing plugins(Update)
○ Fresh import(Delete and replace)

b) Click on Import Button in the Toolbar

c) Import Plugin Configuration Screen will be opened

d) Select an Import Option to specify how the Plugin Configuration should be imported.

- Select 'Import only new plugins(Add)' Option if you want to Import only those plugins from the csv file which are not already in the system
- Select 'Import new and update existing plugins(Update)' Option if you want to Import all Plugins which are only in csv and not in database and update the plugins which are both in csv and database. Plugins, which are only in database and not in csv, would not be changed.
- Select 'Fresh Import(Delete and replace)' Option to clean the database and Import all the plugins from the csv file

e) Browse the csv file

f) Click Import

g) Plugins would be imported according to the selected option

Using ant target

a) Login to nsp-primary box using tekelec user

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

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

where,

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

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

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

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

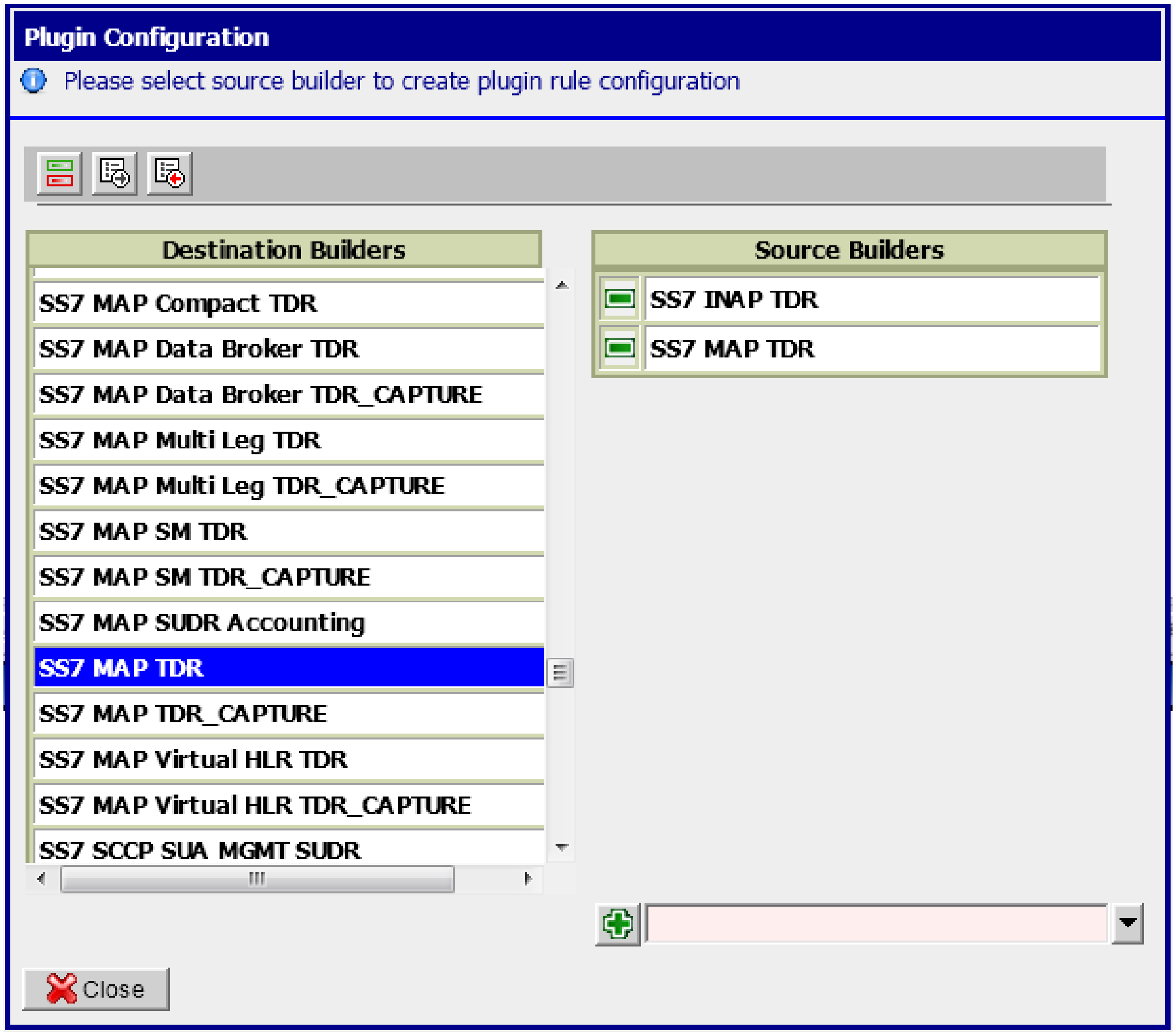
Toggle View Option 'Switch between Source and Destination View'

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

b) Click on Toggle Button in the Toolbar

c) The Plugin Display View will change from Source → Destination to Destination → Source

d) Plugins and Plugin Rules can be Added/Deleted/Updated as explained, but the view display in this case will be Destination Builder → Source Builder for Plugins and Destination EPI → Source EPI in case of Plugin Rules. There will be no change in the software behavior except the view.



Plugin Configuration

Please select source builder to create plugin rule configuration

Destination Builders
SS7 MAP Compact TDR
SS7 MAP Data Broker TDR
SS7 MAP Data Broker TDR_CAPTURE
SS7 MAP Multi Leg TDR
SS7 MAP Multi Leg TDR_CAPTURE
SS7 MAP SM TDR
SS7 MAP SM TDR_CAPTURE
SS7 MAP SUDR Accounting
SS7 MAP TDR
SS7 MAP TDR_CAPTURE
SS7 MAP Virtual HLR TDR
SS7 MAP Virtual HLR TDR_CAPTURE
SS7 SCCP SUA MGMT SUDR

Source Builders
SS7 INAP TDR
SS7 MAP TDR

Configure Mail Server (Optional)

This procedure describes how to configure the SMTP mail server on Oracle Linux platform.

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

1. Open a terminal window and log on as root on Standard Server
2. Edit hosts file and make an entry of mail. Server as shown below:

```
# vi /etc/hosts

10.248.18.4              mail.server
```

Output of hosts file will be similar as shown below. Replace 10.248.18.4 with your mail server IP

```
# cat /etc/hosts
```

```
10.248.18.4                    mail.server
```

Configure Authenticated Mail Server (Optional)

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

Note: This procedure is performed after the SMTP has been configured.

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

1. Connect to the NSP application interface.

2. Log in as weblogic on the WebLogic Console.

3. Select **Services ► Mail Sessions ► NspMailSession.**

4. Click **Lock&Edit** and modify the JavaMail properties as needed. For example:

   ```
   mail.transport.protocol=smtp,
    mail.smtp.host=mail.server,
   mail.smtp.from= noreply@tekelec.com,
   mail.smtp.timeout=5 00,
   mail.smtp.connectiontimeout=500
   ```

5. Add the following parameters:

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

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

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

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

7. Click **Save.**

8. Click **Activate Configuration.**

9. Log in as root on the Management server and run:

   ```
   # service nspservice restart
   ```

Configure SNMP Management Server (Optional)

This procedure describes how to configure the SNMP on management server in Oracle Linux Platform.

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

1. Log in as root user on the Standard Server and run below mentioned script.

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

   This script will prompt for SNMP server IP. If no argument is provided in the script then by default SNMP V3 will be configured. If version V2 or v2 is passed then SNMPv2 will be configured. The script shall update the configuration in /etc/snmp/snmpd.conf file

2. Restart the jmx agent service.

```
# systemctl enable snmpd;service jmxd restart
```

Note: It must be made sure that alias 'localhost" is pointing to Management Server IP address in /etc/hosts file on management server. If not then create or modify alias to point to Management Server IP address and restart jmx agent. Example below with mgmt as NSP host name.

```
# cat /etc/hosts

10.11.12.13 mgmt localhost
```

Modify WebLogic Administration Password (Optional)

Weblogic is installed on a Standard Server with 10.4.0 Release. The following steps must be executed to change the weblogic administration password:

1) Log on to management server as root user and execute below script

```
# /opt/nsp/scripts/procs/nsp_update_proc.sh wlsPasswordConfiguration <NEW PWD> <OLD PWD>
```

This script shall required old password and new password for weblogic. The script shall take around 45 – 60 mins for completion and restart nspservice twice.

Configure Session Timeout (Optional)

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

1. Log in as TklcSrv on the NSP application interface.
2. Select the **Security** application.
3. Select **Action ► Manage Tokens.**

   The Tokens window appears.
4. Type the appropriate value (in minutes; must be from 15 to 480, e.g., 30) in the **Session timeout** field and click **Apply.**

Configure External LDAP (Optional)

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

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

```
# cd /opt/nsp/scripts/procs

# sh nsp_update_procs.sh externalLDAP true
```

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

   http://192.168.1.1/console

   where 192.168.1.1 is the IP address of the Management server.
4. Log in to the WebLogic Console as weblogic.

5. Select **Security Realm** ► **myrealm** ► **Providers** ► **Authentication**.
6. Click **Lock&Edit** and add a new LDAP Authenticator.

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

To View the user locked icon and unlock feature for an External LDAP user in NSP GUI(Security):

1. Select **Security Realm** ► **myrealm** ► **Configuration** ► **General** ► enable "**Use Authorization Providers to Protect JMX Access**"
2. Select **Security Realm** ► **myrealm** ► **Configuration** ► **General** ► enable "**Automatically Restart After Non-Dynamic Changes**"
3. Select **Security Realm** ► **myrealm** ► **Realm Polices** ► **JMX Policy Editor**
4. Click on **Next**, Select **ALL BEANS TYPE** ► **weblogic.management.runtime** ► **UserLockoutManagerRuntimeMBean** ► **Next**
5. Select **Lookup Operations: Permission to Invoke** ► **Create Policy** ► **Add conditions** ►
6. In Predicate List, select '**Allow Access to everyone**' ► Finish ► **Save**
7. Go to back to **ALL BEANS TYPE** ► **weblogic.management.runtime** ► **UserLockoutManagerRuntimeMBean** ► **Next** as in step 2
8. Select **Attributes: Permission to Read** ► **Create Policy** ► **Add conditions** ►
9. In Predicate List, select '**Allow Access to everyone**' ► **Finish** ► **Save**
10. Go to back to **ALL BEANS TYPE** ► **weblogic.management.runtime** ► **UserLockoutManagerRuntimeMBean** ► **Next** as in step 2
11. Select **Operations: Permission to Invoke** ► **Create Policy** ► **Add conditions** ►
12. In Predicate List, select '**Allow Access to everyone**' ► **Finish** ► **Save**

Configure the default settings for the new users (Optional)

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

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

Configure CSV streaming feed feature (Optional)

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

1. Open a terminal window and log in as tekelec on the Management server Admin Server
2. Run the appropriate commands:
   - To enable CSV streaming feed, run:

     ```
     # cd /opt/nsp/nsp-package/framework/core

     # ant enable.csv.license
     ```
   - To disable CSV streaming feed, run:

```
# cd /opt/nsp/nsp-package/framework/core

# ant disable.csv.license
```

Configure FSE automated update (Optional)

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

NSP SCAN REGURLARLY DEFINED FOLDER AND ITS SUBFOLDER (EVERY 30 MIN) TO FIND FILES WITH SAME NAME AS THE THOSE DECLARED. IN THIS CASE IT LOADS FILE TO REPLACE EXISITING FSE AND REAPPLY IT AUTOMATICALLY TO SELECTED SESSION.

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

   The Enrichment Files List screen opens
4. Click on automated update button in list toolbar.

   The FSE Auto Update Configuration screen opens.
5. ENTER SFTP LOCATION WHERE SYSTEM CAN FIND ENRICHMENT FSE FILE.

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

   - <USER> IS USERNAME OF SFTP SERVER
   - <PASSWORD> IS PASSWORD OF SFTP USER
   - <HOSTNAME_OR_IP> IS ADDRESS OF SFTP SERVER
   - <PATH> IS RELATIVE PATH UNDER USER HOME FOLDER IN SFTP SERVER

   Note: Empty string turns off automated update
6. CLICK OK TO VALIDATE CHANGES.

Configure NSP FTP or SFTP Server

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

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

   a. Open a terminal window and log in as root on the Management server
   b. As root, run:
   ```
   # cd /opt/nsp/bea/user_projects/domains/tekelec/nsp
   ```
   c. Copy the contents of file sftp_security.pub.

2. **Update the FTP or SFTP server**

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

Do not use root user to transfer files. tekelec and other users should be use.

By default, files will be uploaded to user home. E.g- /opt/nsp for tekelec

Modify Database Password

The procedure is needed to be executed in following scenarios:

- Password Change of Management Database user
- Password Change of Data Record Storage Database user
- Adding a new Data Record Storage Server in an existing site or a new site
- After Major upgrade to 10.2, so that wallet for database user is generated and sync to various susbsystem(s)

1. Log on to management 1box as root user.
2. Execute below commands

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

The script will ask for below parameters:

a. Database User Name e.g. “NSP” for management database or “IXP” for Data Record Storage Server database
b. Service Name e.g. “NSP” for management database or “IXP” for Data Record Storage Server database
c. Database Server IP Address : IP Address of the server where the database is hosted.
d. Old Password of database user
e. New Password to be set: It can be same as old but the script shall warn the user for new and old password being same.
f. Confirmation of new password
g. Wallet Password: Take the wallet password from database administrator
h. Password of “sys” user : Take the sys user password from database administrator

Note: During the execution, the script will ask for the root password of mgmt. server and cfguser password of target server for synching credentials with mediation and acquisition servers discovered in the various sites managed on this management server. The password for cfguser user shall be asked only for the server(s) on which the ssh keys are not already shared between tekelec and cfguser.

Sync Database Credentials

The procedure is needed to be executed in following scenarios:

- A new server is added into an Acquisition Subsystem
- A new server is added into a Mediation Subsystem

1. Log on to management server as root user.
2. Execute below commands

```
# su - tekelec
# cd /opt/nsp/scripts/oracle/cmd/
# sh syncFiles.sh
            Or
# sh syncFiles.sh <IP1>
            Or
# sh syncFiles.sh <IP1> <IP2> ……….. <IPn>
```

The script if not provided any argument should perform the sync of credentials to the entire server discovered in various sites managed by the management server.

If the script is executed with one or more IP address (separated by space), then credentials shall be synced to all the IP address passed as arguments.

Note: During the execution, the script will ask for the root password of mgmt. server and cfguser password of target server for synching credentials with mediation and acquisition servers discovered in the various sites managed on this management server. The password for cfguser user shall be asked only for the server(s) on which the ssh keys are not already shared between tekelec and cfguser.

Modify Wallet Password

The procedure should be executed in case user want to modify the password for wallet.

1. Log on to management server as root user.
2. Execute below commands

```
# cd /opt/nsp/scripts/oracle/cmd
# ./modifyPassword.sh WALLET
```

The script shall prompt for the following:

- The old password: the existing wallet password.
- The new password: the new wallet password.

Note: During the execution, the script will ask for the root password of management server and cfguser password of target server for synching credentials with mediation and acquisition servers discovered in the various sites managed on this management server. The password for cfguser user shall be asked only for the server(s) on which the ssh keys are not already shared between tekelec and cfguser.

SRDC – How to Collect NSP Logs

Procedure

- Reproduce the issue
- As root, on NSP (Weblogic1 server), run tarNSPLog.sh.

In PIC 10.3, script is stored in /opt/nsp/scripts.

Command Output

Output example (4 box NSP):

```
[root@nsp-primary ~]# ./tarNSPLog.sh
No parameter. Getting 10 days of logs (2014-05-26)
Getting 10 days of logs (2014-05-26)
Processing apache server

Preparing copy of logs          Done.
Creating global tar file ...    Done.
Zipping file ...                Done.
Getting 10 days of logs (2014-05-26)
Processing oracle server
Preparing copy of logs          Done.
Creating global tar file ...    Done.
Zipping file ...                Done.
Processing wls1 server
Preparing copy of logs          Done.
Creating global tar file ...    Done.
Zipping file ...                Done.
Getting 10 days of logs (2014-05-26)
Processing wls2 server
Preparing copy of logs          Done.
Creating global tar file ...    Done.
Zipping file ...                Done.
Four files were created (one per box):
/opt/nsp/tarNSPLogs/NSP_2014-06-05-08_59_log_J2EE_host1.tar.gz
/opt/nsp/tarNSPLogs/NSP_2014-06-05-08_59_log_DB_hosts.tar.gz
/opt/nsp/tarNSPLogs/NSP_2014-06-05-08_59_log_front_end.tar.gz
/opt/nsp/tarNSPLogs/NSP_2014-06-05-08_59_log_J2EE_host2.tar.gz
```

The script is getting 10 days of log history by default (ie. log files with modified date in last 10 days if available). This can be overridden by adding number of days to the command (if logs are available).

Gathered files

Script gathers the following directories:

- Product version
- Weblogic instances logs
- Access and error log from Apache
- Jmx logs and configuration
- Oracle database bdump and listener log
- sar files (system activity)
- Purge job logs
- Backup log
- Partition space usage
- Memory usage
- Running processes

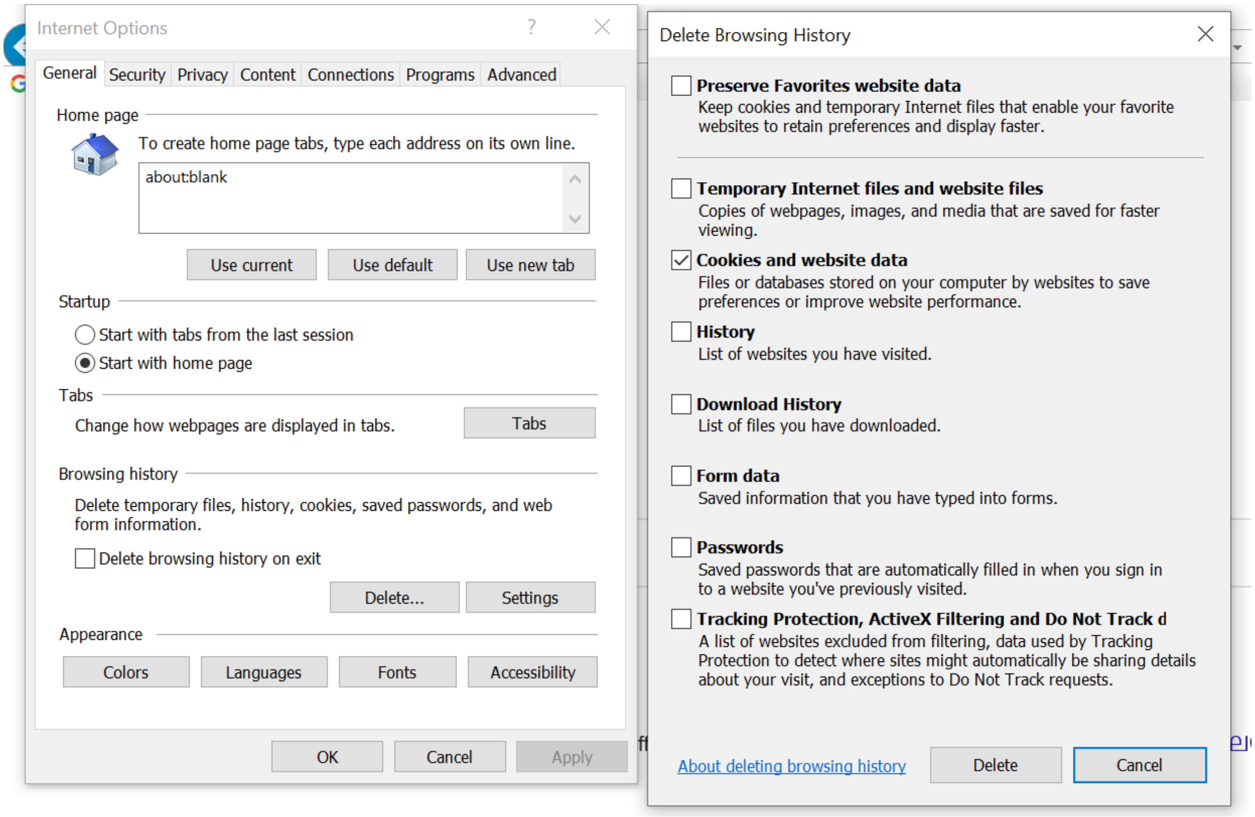
and add them in a .tar.gz file name with time and date.

Secure,HttpOnly flag in Cookies(Mandatory)

For Https access to nsp the Secure and HttpOnly flag has been set in cookies, hence everytime while switching in between Http and Https version of the Management Server or Weblogic Console, the cookies has to be cleared using the following process.

The following is the process for Internet Explorer

Tools → Internet Options →Delete→Cookies and website data→Delete→Apply→Ok



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Home page

To create home page tabs, type each address on its own line.

about:blank

Use current | Use default | Use new tab

Startup

○ Start with tabs from the last session

● Start with home page

Tabs

Change how webpages are displayed in tabs. Tabs

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Delete... | Settings

Appearance

Colors | Languages | Fonts | Accessibility

OK | Cancel | Apply

Delete Browsing History

□ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

□ **Temporary Internet files and website files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies and website data**
Files or databases stored on your computer by websites to save preferences or improve website performance.

□ **History**
List of websites you have visited.

□ **Download History**
List of files you have downloaded.

□ **Form data**
Saved information that you have typed into forms.

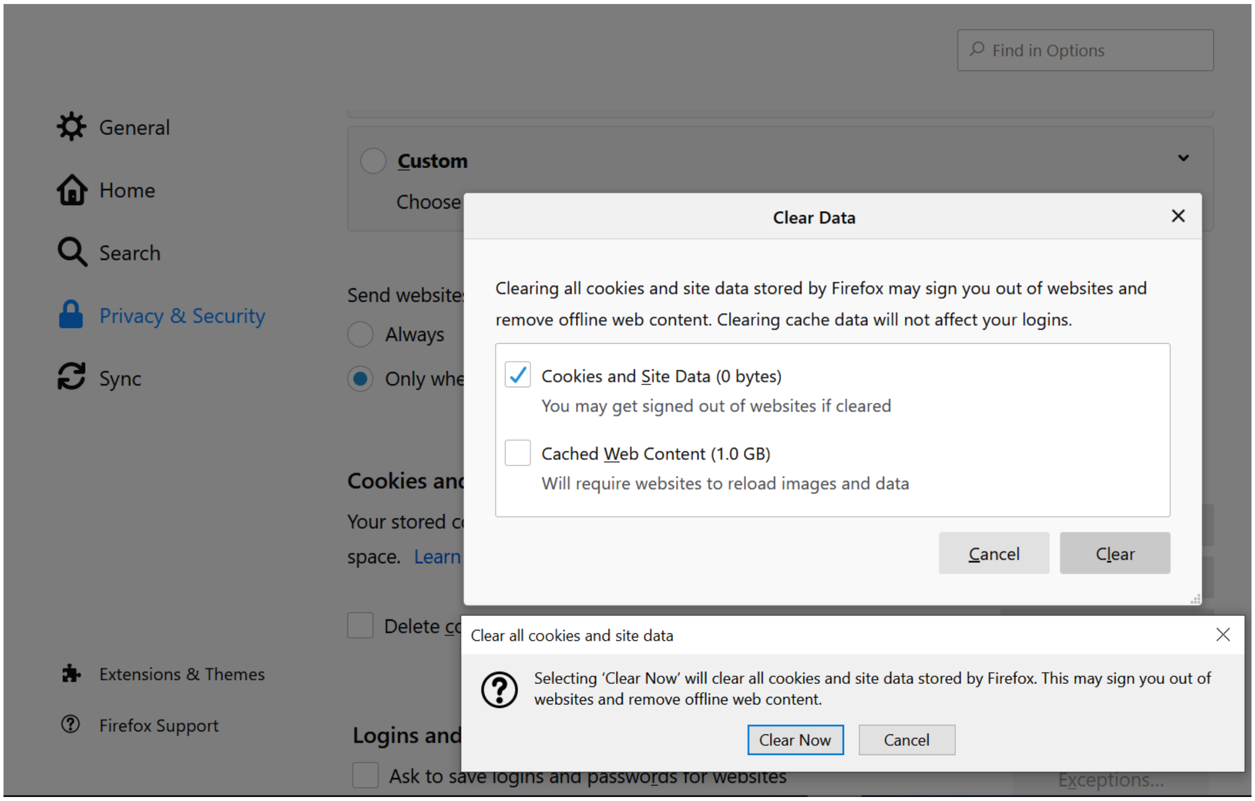
□ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

□ **Tracking Protection, ActiveX Filtering and Do Not Track d**
A list of websites excluded from filtering, data used by Tracking Protection to detect where sites might automatically be sharing details about your visit, and exceptions to Do Not Track requests.

About deleting browsing history | Delete | Cancel

The following is the process for Mozilla Firefox

OpenMenu→Options→Privacy and Security→Clear Data→Cookies and SiteData→Clear→ClearNow



Clear Data

Clearing all cookies and site data stored by Firefox may sign you out of websites and remove offline web content. Clearing cache data will not affect your logins.

☑ Cookies and Site Data (0 bytes)
You may get signed out of websites if cleared

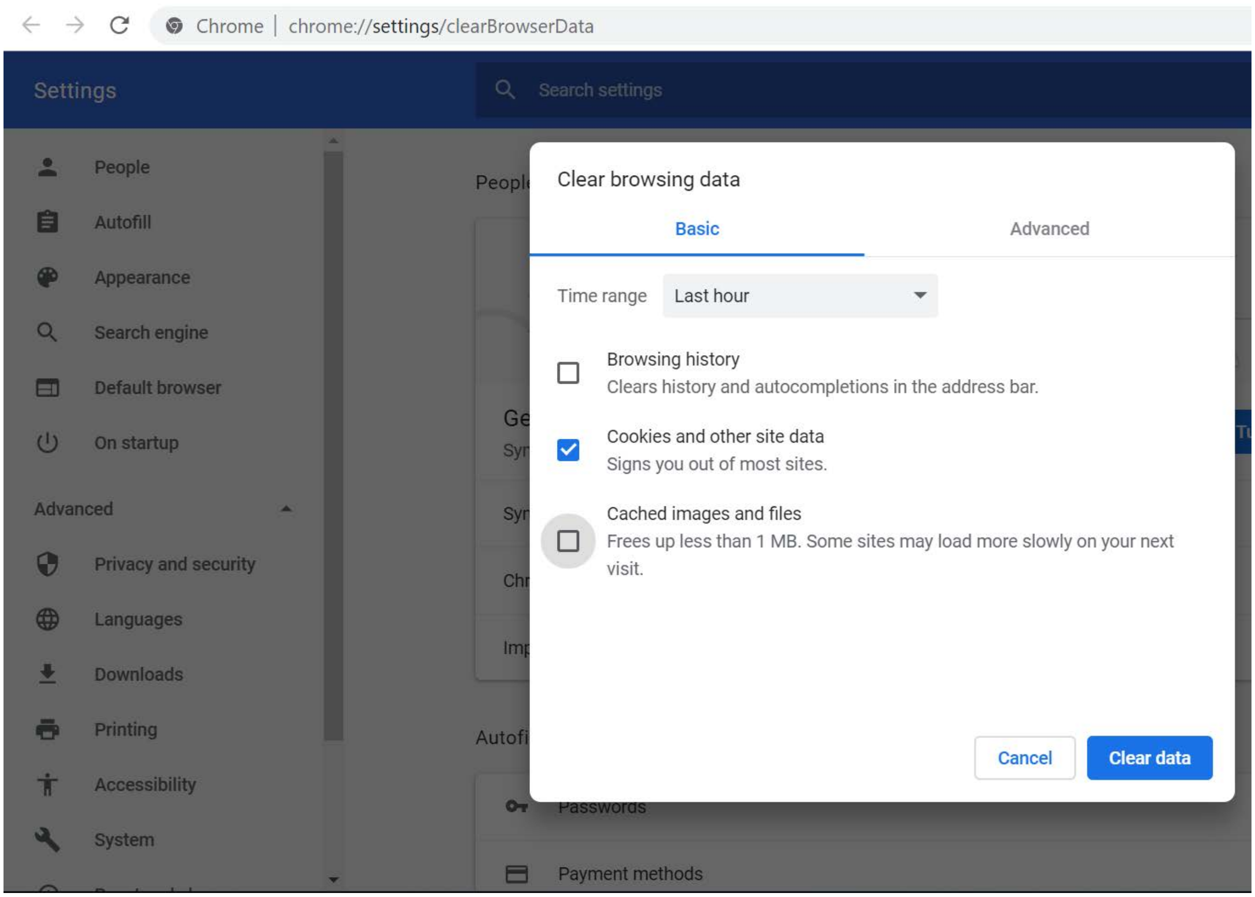
□ Cached Web Content (1.0 GB)
Will require websites to reload images and data

Clear all cookies and site data

Selecting 'Clear Now' will clear all cookies and site data stored by Firefox. This may sign you out of websites and remove offline web content.

The following is the process for Chrome Browser.

Ctrl+H→Clear Browsing Data→Cookies and other site data→clear data



Clear browsing data

Basic | Advanced

Time range: Last hour

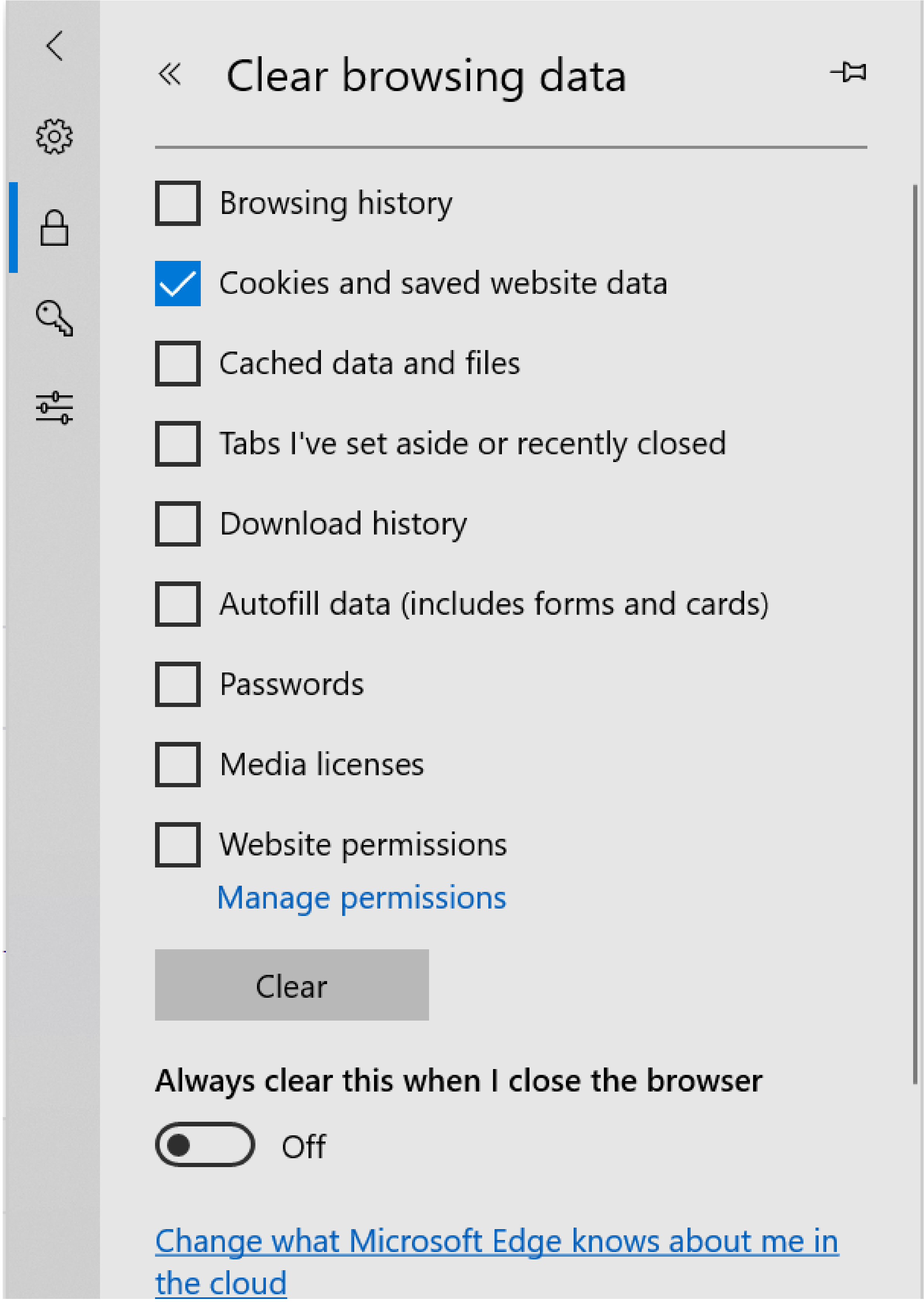
☐ Browsing history
Clears history and autocompletions in the address bar.

☑ Cookies and other site data
Signs you out of most sites.

☐ Cached images and files
Frees up less than 1 MB. Some sites may load more slowly on your next visit.

The following is the process for Edge Browser

Ctrl+H→Clear History→Cookies and saved Website Data→Clear



Clear browsing data

□ Browsing history

☑ Cookies and saved website data

□ Cached data and files

□ Tabs I've set aside or recently closed

□ Download history

□ Autofill data (includes forms and cards)

□ Passwords

□ Media licenses

□ Website permissions

Manage permissions

Clear

Always clear this when I close the browser

○ Off

Change what Microsoft Edge knows about me in the cloud

8. Acquisition Maintenance Procedures

Procedure to enable/disable timestamp resolution to nanoseconds

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

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

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

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

After modification of this parameter, the Probed pduServer0 process must be restarted.

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

Falco Firmware upgrade procedure

Use the MOS Note How to Update Falco Firmware Doc Id 2026088.1, at the end of the procedure, displayed version must be:

```
Version:  1.00i

FPGA V5:  C3090111

         0F120005

FPGA V4:  C1072711

         0F121E04
```

Add New Server in the Integrated Acquisition sub-system

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

1. Install Integrated Acquisition server
    a. **Install** the additional Integrated Acquisition server using the procedures mentioned in Chapter 10 in PIC 10.4.0 Installation document .Only procedures till section "Install Acquisition Server Application" should be executed.
    Note: Use the bulkconfig file already present on the already installed servers and add the entry for the additional Integrated Acquisition server in the bulkconfig file. Copied the modified bulkconfig file to all the other Integrated Acquisition servers.

    Run bulkconfig script as root user on all subsystem servers:

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

2. Discover the server on Management Server
    a. **Log in to the Management Server application**
        i. Log in as tekelec to the Management Server application interface using the Management Server IP address.
        ii. Click **Centralized configuration.** The Management Server application launches.
3. Discover the server on Management Server
    a. **Modify Integrated Acquisition site on Management Server**
        i. Select **Equipment Registry ► Sites**
        ii. Navigate to **XMF**
        iii. Right click in the requested subsystem
        iv. Select **Add** from the popup menu.
        v. Fill in the **Host IP Address** field with the IP address of the server you want to add.
        vi. Click the **Create** button.
        vii. Return to the **Equipment registry**.
        Click on the subsystem to display the list of servers.
        viii. Choose the newly added server and press **Discover applications.**
4. **Sync Database Credentials**
    Execute procedure described in section **7.17 Sync Database Credentials**

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

Change the hostname of the Probed Acquisition Server

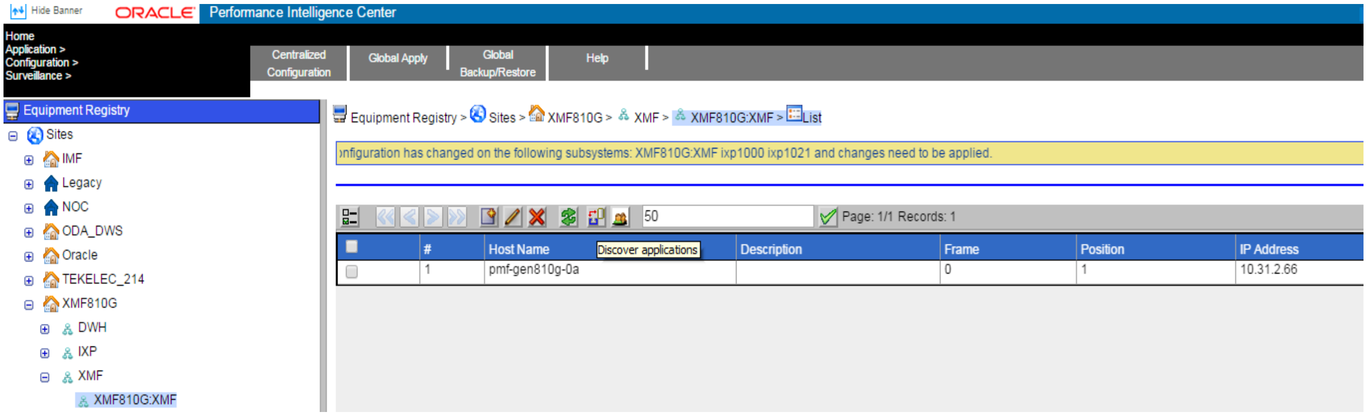
The procedure should be executed for the Probed Acquisition server in case there is a need to change the hostname of the server. Following steps must be executed for changing the hostname of the server:

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

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

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

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



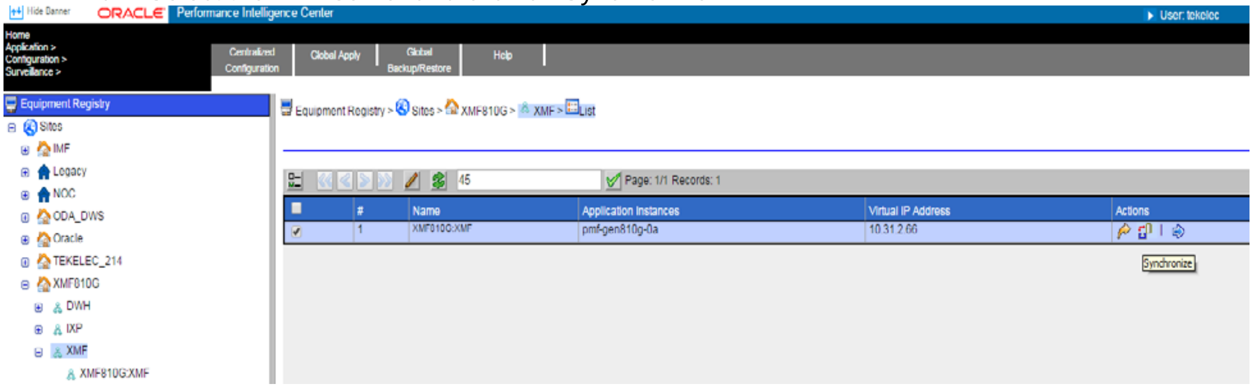
Equipment Registry > Sites > XMF810G > XMF > XMF810G:XMF > List

›nfiguration has changed on the following subsystems: XMF810G:XMF ixp1000 ixp1021 and changes need to be applied.

50 Page: 1/1 Records: 1

□	#	Host Name	Description	Frame	Position	IP Address
□	1	pmf-gen810g-0a		0	1	10.31.2.66

   d. Select the xMF server and click on Synchronize



Equipment Registry > Sites > XMF810G > XMF > List

45 Page: 1/1 Records: 1

□	#	Name	Application Instances	Virtual IP Address	Actions
☑	1	XMF810G:XMF	pmf-gen810g-0a	10.31.2.66	

5. Apply Change
   a. To Apply Changes for each subsystem go to Acquisition ➤ Sites ➤ XMF.
   b. Right click on subsystem and click on Apply Changes option on menu.

Remove Server from the Integrated Acquisition sub-system

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

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

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

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

Update Integrated DSR password in Probed Server

The integrated DSR is using SOAP interface and the APIs are password protected. DSR 8.3 will support the password modification, so PIC should also update the password in its database. The procedure mentioned below is for updating the DSR webservices password in PIC database. The dsrMonitor process on Probe will report following error, in this case password from DSR should be updated on Probe Server.

```
TR-V   Can not get password!!! ERROR:   GN_INTERN:   Decryption finalize failed
```

TR-V DSR Soap Initialization failed

The pre-requisite is to get the new encrypted password from DSR team, after the new password is collected from DSR team perform following steps:

1. Login to Probe server as cfguser
2. ivi SoapSecurityConfig
3. update the password field with new password
4. Save the SoapSecurityConfig table, Enter OK when prompted to apply changes
5. Restart dsrMonitor process using
    a. pm.set off dsrMonitor
    b. pm.set on dsrMonitor

Modify Packet truncation in PMIA module on Probed Server

In Probed acquisition server, the PMIA module enforces the packet truncation for the SCTP and TCP packets. The SCTP as a transport layer is mainly used for the SIGTRAN and Diameter packets, whereas TCP as a transport layer is mainly used for Diameter and HTTP2 packets. The packet truncation is controlled inside the PMIA kernel module by providing few parameters during the initialization of the PMIA module. In case the truncation parameters are required to be changed then the PMIA module should be re-initalized. The maximum packet limit supported by the PMIA is 9000 bytes, any packet more than 9000 bytes is dropped by the PMIA module. The higher packet truncation limit could derate the performance of PMIA filtering and also the network bandwidth as bigger packets would be transferred over DTS. The memory requirement can go also go up.

The packet truncation parameters for the various transport/protocols are configured in the PMIA module using the startup script "pmiaInstall". The script is available at the following path on probed acquisition server:
/etc/init.d/pmiaInstall

The following parameters are provided for packet truncation:

Parameter Name	Default Value (bytes)	Parameter Value Range (bytes)	Description
max_dia_tcp_msg	4096	Minimum: Default value Maximum: 9000	This parameter is for the length of the Diameter packet over TCP transport protocol. Any diameter packet with length more than this value is truncated to the value defined for this parameter. The total reassembled length can't be more than this value.
max_http2_msg	4096	Minimum: Default value Maximum: 9000	This parameter is for the length of the HTTP2 data frame over TCP transport protocol. Any HTTP2 data frame with length more than this value is truncated to the value defined for this parameter. The total reassembled length can't be more than this value.

sctp_chunk_frgt_truncate_len*	4096	Minimum: Default value Maximum: 9000	This parameter is for the length of the SCTP data chunk over SCTP transport protocol. Any data data chunk with length more than this value is truncated to the value defined for this parameter. The total reassembled length of the data chunk can't be more than this value.

Note *: sctp_diameter_avp_reorder_len should be same as sctp_chunk_frgt_truncate_len

The parameters are separated by space, an example is given below:

```
/sbin/insmod $libPath$module.ko    sctp_chunk_reassemble=1 max_tcp_msg=32768 max_dia_tcp_msg=4096
max_http2_msg=4096 sctp_chunk_frgt_truncate_len=4096 sctp_diameter_avp_reorder=1
sctp_diameter_avp_reorder_len=4096 http2_pkt_reassemble=1
```

Procedure to modify the truncation parameters in PMIA

The following procedure should be executed in the maintenance window as it will involve kernel modules *pmia & af_pmia* to restart along with the user space *pmiaMonitor* process.

1. As cfguser, stop pmiaMonitor process using "*pm.set off pmiaMonitor*"
2. Switch user to "*root*" using "su –"
3. Stop pmia module using "*service pmiaInstall stop*"
4. Edit */etc/init.d/pmiaIntall* script using vi editor and modify the truncation parameters as required. For example max_dia_tcp_msg=5000
5. Save the */etc/init.d/pmiaIntall* script
6. Start the pmia module using "*service pmiaInstall start*"
7. Switch user to "*cfguser*", using *"su – cfguser"*
8. Edit *LongParam* table using "*ivi LongParam*" and modify "*PmFrSize*" parameter to at least the same value as the modified truncation parameter value.
9. Save the *LongParam* IDB table and write "y" when asked to apply change

APPLY THE CHANGES [yn]?

10. Restart pmiaMonitor process using "*pm.set on pmiaMonitor*"
11. Verify the traffic monitoring.

Note: In case the values for the various truncation parameter are different then value for PmFrSize in the LongParam should be set at least equal to the largest value set for the various truncation parameter. For example max_dia_tcp_msg=4096 and max_http2_msg=5000 then PmFrSize should be set at least 5000 in LongParam. PmFrSize value can't be more than 9000 bytes. A clobber on the Acquisition server will reset the default value(4096) of PmFrSize parameter, so care must be taken to update the value again after the clobber of IDB.

9. Mediation Maintenance Procedures

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

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

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

Offload DFPs from the Mediation Server

This procedure describes how to offload the dataflow processing from the Mediation server. The procedure can be executed during the maintenance procedure or when the server is under heavy load. The capacity management session (Refer to Capacity Management Good Practices in the Chapter 9) should be used to find the load on the system and accordingly the decision to offload DFPs should be made.

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

2. **Redistribute DataFeed**
    a. Navigate to Management Server home page
    b. Click on **DataFeed**.
    c. Open the **DataFeeds** tree and select **xDR/KPI exports**.
    d. Deactivate all the processes that are assigned to the particular server by clicking on **Deactivate.**
    e. Wait until feed is deactivated.

    f. If possible, click on **Edit** button and redistribute such processes on the other servers by choosing new **Host name** and clicking on **Finish**.
    g. If the **Edit** button will not be visible, (in the case that feed status will be **Unknown** or **Recovering**) click on **Copy feed** and create a new feed with the same behavior on the new server. As soon as possible, remove the old feed by **Delete** button.

3. **Cancel KPI historical tasks**
    a. Go to the Management Server home page
    b. Navigate to the **ProTraq** application in the Management Server.

c. Open **Historical task** tab.

d. Cancel all the tasks that are assigned to the particular server.

4. **Reassign external connections**

Note: The steps before take care about the stream tracking and if a producer dataflow processing has moved to another server, the consumer dataflow processing will finish processing the buffered data on the first server and automatically reconnect on the newly assigned server. However, this automatic procedure does not apply to external connections.

a. Acquisition probe (Integrated Acquisition, Probed, MSW) sending data to a stream on this machine. In such a case it is required to reconfigure also this system in order to reconnect to the replacement (in general the spare) server

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

c. Queries.If the relevant server was used as the server answering to the queries, the subsequent connections will fail until this server has finished its maintenance. If this period will be long, you must configure a new address for queries

Configure PDU Storage Parameters

a) Log into any server from Mediation subsystem

b) As cfguser run:

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

Example output:

```
ixp7000-1a StbMaster

ixp7000-1b ActMaster

ixp7000-1c Slave
```

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

c) On ActMaster server, type:

```
$ ivi SubsystemTaskParam
```

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

```
#!/bin/sh

iload -ha -xU   -fID -fParamName -fParamValue SubsystemTaskParam \

<<'!!!!'

1|AlarmClear|1500

2|AlarmFail|1500
```

```
3|MaxFileAge|864000
4|MaxPercentUsage|90
5|ExcludePath|write.enable
6|Path|/opt/TKLCixp/pdu
7|Interval|5
8|Interval|300
9|Path|/es
10|ExcludePath|statistics
11|LoginName|ixp
13|AlarmFail|100
14|AlarmClear|100
15|OracleMaxPurgeTime|900
16|IdbPurgeTime|21600
17|TaskPurgeTime|604800
18|ExcludePath|run
19|DatabaseName|ixp0008-1a_DWH
20|HostName|ixp0008-1a
21|Password|IXP
!!!!
```

Change the value of parameter **MaxFileAge** (864000 seconds, in this example).

Don’t forget to save the change when quitting the editor.

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

```
$ pm.kill IxpPurge
```

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

Enable/disable Write Access to the PDU Mounts

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

Enable/disable Write Access to the PDU Mounts for TPD based storage

1. **To disable writing**

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

   ```
   # su - platcfg
   ```

   b) Navigate to **IXP Configuration** ➤ **PDU Storage** and press **Edit**

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

2. **To enable writing**

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

   ```
   # su - platcfg
   ```

   b) Navigate to **IXP Configuration** ➤ **PDU Storage** and press **Edit**

   c) Mark both PDU mounts to **yes** to enable writing.
   Note: After this step, the IxpBuild processes will be able to write to its PDU mounts from a specific PDU Storage Server.

Enable/disable Write Access to the PDU Mounts for non TPD based storage

1. **To enable writing**

For ZFS and Standard storage, following should be done to enable Write access for PDU mounts.

As root user on mediation server, change directory to PDU mount directory

```
# touch write.enable
```

2. **To disable writing**

For ZFS and Standard storage, following should be done to disable Write access for PDU mounts.

As root user on mediation server, change directory to PDU mount directory

```
# rm write.enable
```

Set Behavior Mode for Data Record Storage Server

This procedure describes how to set the behavior mode for a specific Data Record Storage Server that is part of the Dara Record storage pool.

In case of single Data Record Storage server in a storage pool, the following steps will not avoid data loss, as there is no other server to store the xDR.

In this case, you may edit the DFP store and select another storage pool...

a. Open a web browser and log in to Management Server application interface.
b. Click on **Centralized Configuration**.
c. Navigate to **Mediation** ➤ **Sites** ➤ **IXP subsystem**
d. Click on **Storage**.
e. In the list in the right, choose one of the three possible states: **ACTIVE**,

MAINTENANCE, and QUERY ONLY.

f. Right click on the Mediation subsystem and press **Apply Changes**.

Re-Sync the Mediation Configuration

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

1. **Drop synchronization history on the Mediation ActMaster server**

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

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

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

2. **Run Apply Changes to Mediation subsystem from Management Server**

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

Add Server to the Mediation Subsystem

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

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

1. **Integration with the Mediation subsystem**

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

   a) Open a terminal window and log in on Mediation server you are about to add to the Mediation subsystem as root.

   b) Update the /root/bulkconfig file.
   Note: The easiest way to update the bulkconfig file is to copy the bulkconfig file from any server of the target Mediation subsystem. Store this file to new Mediation server. Then add the host line with newly installed Mediation server to the bulkconfig file. Check that the bulkconfig file on the additional Mediation server now contains overall subsystem configuration information and also make sure that the bulkconfig files contains records for all servers in the subsystem including the newly added one.

c) Once your bulkconfig is valid run automated integration script:
Note: This step must be run on additional Mediation server, the one where you have updated the bulkconfig file in previous step.

Run the following steps:

1. As `root` run:
```
# bc_customer_integration.sh --local
```
2. Once finished server will reboot.
3. Log in back to the same newly added server. As `root` run:
```
# /usr/TKLC/plat/sbin/rootSshLogin -permit

# bc_adjust_subsystem.sh
```

d) Run analysis to see if the subsystem has been adjusted properly. As `root` run:
```
# bc_diag_bulkconfig.sh -a
```

2. **Install the xDR Builder package**

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

As `cfguser` run:

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

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

3. **Add server to existing Mediation subsystem**

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

j) Choose the newly added server and press **Discover applications.**

4. **Sync Database Credentials**
Execute procedure **Sync Database Credentials** of chapter 7

5. **Apply configuration to the Mediation subsystem**

a) Navigate to the **Mediation** view.
b) Navigate to **Sites**
c) Open **IXP** and right-click on the subsystem.
d) Select **Apply changes…** from the popup menu.

e) Click on the **Next** button

f) Click on the **Apply Changes** button.

g) Wait until changes are applied.

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

6. **Verify license installation**

a) Log in as cfguser on the Mediation Active Master server.

b) Run:

```
$ IxpCheckLicense
```

c) Verify the output.

The information about the license should state that license is valid and that license type is not STARTUP. If the license type is STARTUP , refer to My Oracle Support

Add Mediation Server to the Mediation Subsystem in Management/CCM

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

1. **Add server to existing Mediation subsystem**

a) Open a web browser and log in to Management Server application interface.

b) Click on **Centralized Configuration**

c) Navigate to **Sites**

d) Navigate to **IXP**

e) Right click in the requested subsystem

f) Select **Add** from the popup menu.

g) Fill in the Host IP Address field with the IP address of the server you want to add.

h) Click the Create button.

i) Return to the **Equipment registry**.
Click on the subsystem to display the list of servers.

j) Choose the newly added server and press **Discover applications.**

2. **Sync Database Credentials**

3. Execute procedure **Sync Database Credentials** of chapter 7

4. **Apply configuration to the Mediation subsystem**

a) Navigate to the **Mediation** view.

b) Navigate to **Sites**

c) Open **IXP** and right-click on the subsystem.

d) Select **Apply changes…** from the popup menu.

e) Click on the **Next** button

f) Click on the **Apply Changes** button.

g) Wait until changes are applied.
h) Verify that result page does not contain any errors.

Remove Server from the Mediation Subsystem

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

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

1. **Offload the Mediation server**
   Offload DFPs from the server you are about to remove from the subsystem. Refer to *Offload DFPs from the Mediation Server*

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

   Shutdown this server. As root run:

```
# poweroff
```

3. **Remove the xDR builders from the Mediation subsystem in Management**
   Note: this step has to be run for the **last server only** of the Mediation subsystem.

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

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

5. **Remove the server from bulkconfig and adjust the subsystem accordingly**
   Note: Run this procedure from ANY Mediation server in the Mediation subsystem BUT NOT from a server you are about to remove.

   a) Open a terminal window and log in to any remaining Mediation server in the subsystem as root.

b) From the bulkconfig file, remove host line with the Mediation server you want to remove from the Mediation subsystem.

c) As root run:

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

# bc_adjust_subsystem.sh
```

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

properly. As root run:

```
# bc_diag_bulkconfig -a
```

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

Change Mediation network interface type to Bonding

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

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

1. **Delete** old interface eth0X
   a. To delete the default route, as root, run:

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

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

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

2. **Configure** the bonding interface
   a. To check if bonding interface exist, as root, run:

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

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

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

   If bonding interface not exist, as root, run:

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

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

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

   d. Restart the network, as root, run:

   ```
   service network restart
   ```

3. In the **bulkconfig** file, be sure to use the bond0 interface (and not the usual ethxx interface)
   a. Login to the iLO as root of any IXP server in the subsystem you are about to reconfigure
   b. Update the /root/bulkconfig file with the new interface

4. Run **Apply change** procedure
    a. Run the IXP subsystem customer integration procedure as root:

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

# bc_customer_integration.sh
```

Installation of External Datawarehouse

Refer to Chapter 6 PIC Data WareHouse Server (DWS) on Third-Party Server in PIC 10.4.0 Installation Guide

Setup NFS Mount for DataFeed Application on Customer Provided Server

Setup NFS Mount for DataFeed Application on TPD based platform

This procedure describes the steps how to setup the nfs mount for Data Export on the customer provided server.

In some cases, the customer did not get an Export Server added to the Mediation subsystem, so the traditional method is still used. UID for cfguser is 2000. The customer must change the UID on their server to allow cfguser to mount and access the filesystem.

Note: UNIX like system is expected to be installed on customer provided server.

1. **Create cfguser user and cfg group**

   Note: Run this step on customer provided server. No exact steps are provided. This differs from system to system.

   - UID for cfguser must be 2000
   - GID for cfg must be 2000

2. **Create export directories**

   Note: Run this step on customer provided server.

   Open a terminal window and log in as cfguser. As cfguser run:

```
$ mkdir -p /es/es_1

$ mkdir -p /es/es_2

$ chmod -R 750 /es
```

   Make sure that the owner of these directories is cfguser and group cfg.

3. **Update the /etc/exports file**

   Note: Run this step on customer provided server.

   Add the following lines into the /etc/exports file

```
/es          ixp????-??(rw,async,no_root_squash,anonuid=-1)
```

```
/es/es_1 ixp????-??(rw,async,no_root_squash,nohide,anonuid=-1)

/es/es_2 ixp????-??(rw,async,no_root_squash,nohide,anonuid=-1)
```

4. **Restart the NFS service**

   Note: Run this step on customer provided server. This step might be platform dependant. Check before executing this step.

   As root run:

```
# service nfs stop

# service portmap restart

# service nfs start
```

5. **Update the /etc/hosts**

   Note: Run this step on customer provided server.

   Add all the Mediations that will use this server as an export target into the /etc/hosts file. Only those machines that will be present in /etc/hosts file and will pass the ixp hostname mask will be able to use this server as an export server.

6. **Configure the DataFeed Application (Management Server)**

   Note: Run this step in DataFeed application (under Management Server).

   Follow with standard DataFeed configuration. Set export server IP to the IP of the machine you just configured, set remote filesystem to /es/es_1 or /es/es_2 and set remote directory to the desired directory name that will be created under /es/es_?/.

Setup NFS Mount for DataFeed Application on Standard Platform

The procedure to install and configure the NFS mounts for data export is similar to the one mentioned below, however the mount points should be created with below information

As cfguser,

```
$ mkdir -p /es/es_1

$ mkdir -p /es/es_2

$ chmod -R 750 /es
```

Refer to Chapter 7 **Packet Data Unit Storage (PDU)** on Third-Party Server in PIC 10.4.0 Installation Guide

Configure the DataFeed Application (Management Server)

Note: Run this step in DataFeed application (under Management Server).

Follow with standard DataFeed configuration. Set export server IP to the IP of the machine you just configured, set remote filesystem to `/es/es_1` or `/es/es_2` and set remote directory to the desired directory name that will be created under /es/es_?/.

External Storage Configuration using NFS on ODA

The external storage can be configured on the ODA for the PDU storage using NFSv4 on the Mediation Servers instead of using a dedicated server.

Procedure to configure NFS mount point on ODA Oracle Server:

1. **Create PDU storage directories as root user**

```
# cd /cloudfs
# mkdir -p    export/pdu_1
# chmod 766 /cloudfs/export/pdu_1
```

2. **Update the /etc/exports file as root user**
Add the following lines into the /etc/exports file

```
/cloudfs/export/pdu_1    ixp????-??(rw,async,no_root_squash,anonuid=-1)
```

3. **Update the /etc/hosts**
Note: Run this step on ODA oracle server.

Add all the mediation servers that will use this server as external PDU storage target into the /etc/hosts file. Only those machines that will be present in /etc/hosts file and will pass the ixp hostname mask will be able to use this server as an external PDU storage server.

As root, edit the /etc/hosts file using vi editor and add the following line for all the mediation servers. Save the file after modification.

```
<ip_address>                    <mediation_server_hostname>
For example
10.31.2.61              ixp9010-1a
10.31.2.62              ixp9010-1b
```

4. **Restart the NFS service**
As root run:

```
# service nfs stop
# service portmap restart
# service nfs start
```

5. **Update bulkconfig**
Edit the bulkconfig file, add the lines starting with the pdu keyword, followed by the IP of the PDU storage server. As root, adjust the subsystem PDU settings with the following command:

```
# bc_adjust_subsystem.sh
```

Data Record Storage installation on HP

The procedure given below is applicable to both RMS and blades for DRS installed before PIC 10.4.0.

Refer and follow the flow defined in Section **2.7 "DWS DL360/BL460 Gen8"** in PIC 10.1 INSTALL DOCUMENT Doc ID E53508 for the Data Record Storage Server installation on Blades and RMS HP hardware. The software release of PIC 10.1 must be used for this installation.

Data Record Storage Post-Integration Configuration

The procedure is applicable for both ODA as well as HP based Data Record Storage Server.

Activate Session Compression

This procedure describes how to activate/deactivate compression for a particular Oracle session.

Before performing this procedure, be aware of the following facts:

- Activated compression will have negative influence on storage speed rate.
- Activated compression will have negative influence on ProTrace queries speed rate.
- Activated compression will have positive influence on storage size.
- All current benchmark tests have been tested with deactivated compression.

Note: Execute this procedure for all Data Record Storage Server servers in the Storage Pool where the session is located, from any remote mediation base server.

1. Login to the any mediation server

   a) Open a terminal window and log in to the mediation server as cfguser.

   b) Navigate to /opt/TKLCixp/prod/db/tuning/cmd directory. As cfguser run:

   ```
   $ cd /opt/TKLCixp/prod/db/tuning/cmd
   ```

2. How to activate the compression

   To activate compression for particular session as cfguser run:

   ```
   $   ./TuningPackage.sh ixp/ixp@<IP>/ixp -c <session>
   ```

   where <IP> is the iP of Data Record Storage server and <session> is the name of particular session.

3. How to deactivate the compression

   To deactivate compression for particular session as cfguser run:

   ```
   $   ./TuningPackage.sh ixp/ixp@<IP>/ixp -x session
   ```

   where <IP> is the iP of Data Record Storage server and <session> is the name of particular session.

4. Verify the settings

   Verify the session list where the session compression is activated. As cfguser run:

   ```
   $   ./TuningPackage.sh ixp/ixp@<IP>/ixp -l
   ```

   Where <IP> is the iP of Data Record Storage server.

All session with activated compression will be listed in the command output.

Capacity Management Best Practices

Purpose

Capacity Management is a set of resources for PIC system self-surveillance. It is only focused on collecting and presenting metrics. This document explains the best practices to use the available data at best to monitor the system and optimize its operation.

Scope

This document describes Capacity Management main lines in order to analyze data provided to manage efficient system audits and troubleshooting.

Capacity Management works on PIC system from release 10.0.

This document is intended for use by internal Oracle personnel trained in software installation on rackmount and c-class blades system, trained Distribution Partners and trained Customer representatives

Software

At PIC software installation, Capacity Management related KPIs are deployed.

- All elements such as dedicated streams and DataFlows for the basic statistical session (CapacityManagement) are automatically created as part of system deployment. The basic statistical session is gathered by the dedicated builder Generic FlowMonitor Stats.
    - Naming convention makes that needed elements will contain CapacityManagement in the name (generally as suffix).
- Each time new equipment such as IXP or xMF 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.
- 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.

No other additional software DVD or ISO file is required.

Licenses

No specific licenses are required for Capacity Management usage, even for the dedicated builder.

Hardware

N/A

Acronyms

Acronym	Description
CCM	Centralized Configuration Management
IXP	Integrated xDR Platform
Kbps	Kilobits per second (throughput)
Mbps	Megabits per second
KPI	Key Performance Indicator
NSP	Network Software Platform
PDU	Protocol Data Unit
PIC	Performance Intelligence Centre
RTU	Right To Use (licensed bandwidth to customer)
TC	Traffic Classification
XB	xDR Builder
xDR	Call Details Record, Transaction Details Record, Session Details Record, ….
xMF	Integrated Message Feeder (IMF) or Probed Message Feeder (PMF)

Terminology
Collection point

It is a "software module" inside the PIC system in charge of processing a stream of data (e.g. PMIA, XB, KPI, LINK, etc.). This module will also provide bandwidth measurements for this feature.

To allow flexibility, this information is not defined as a list in the dictionary, but as a string. This allow to add, modify remove easily *Collection Points* that can be managed by the builder.

A list of currently defined *Collection Points* is displayed in a table in ***Main Description*** section of this document.

Items

Defines a generic format for measurements and therefore uses the word ***Items***to designate a counter that may show the number of frames, events, PDU, xDR, KPI, etc. depending on the category of measurement.

Workload

Based on the same approach of a generic results record, the counter named ***Workload*** can show the number of PMIA patterns applied to properly classify incoming traffic as well as the number of Filter conditions in a ProTraq or the number of mapping access in a static enrichment.

Operations

Based on the same approach of a generic results record, the counter named Operations can show either the number of PMIA patterns applied to properly classify incoming traffic as well as the number of Filter conditions in a ProTraq or the number of mapping access in a static enrichment.

Change Default Passwords of Oracle Accounts (optional)

Refer Modify Database Password

10. External Software Configuration

Java Runtime settings

Refer to PIC 10.4.0 Quick Start Guide

IE Browser Settings

Refer to PIC 10.4.0 Quick Start Guide

11. Knowledge Base Procedures

How to mount the ISO file via iLO

Note: For latest procedure to mount ISO corresponding to iLO4, please refer Doc Id E53486 Platform Configuration Procedure

1. Store the ISO file to the local disk.
2. Open a web browser and enter the IP address of server ILO. After security exception a login page will appear. Log in as root.
3. Navigate to the Remote Console tab.
4. Click on Integrated Remote Console.
   An Integrated Remote Console window appears.
5. Click on Virtual Media which is visible in blue bar at the top of the Integrated Remote Console window.
6. Navigate to Image with a small CD-ROM picture on the left side. Click on Mount.
   A window will pop up asking for the ISO path. Navigate to the ISO file and click Open.
7. Now the ISO file is mounted on a target server as a virtual CD-ROM. Such new device will appear under /dev/ directory.
   To find the new virtual CD-ROM media run on a target server as root:

```
# getCDROMmedia
```

This will list a virtual CD-ROM media devices with the exact device name.
Example output:

```
[root@ixp1977-1a ~]# getCDROMmedia

HP Virtual DVD-ROM:scd0
```

This record denotes virtual CD-ROM device /dev/scd0 ready for any other operation.

Configure and Verify ILO Connection

Note: For latest procedure to configure iLO, please refer Doc Id E53486 Platform Configuration Procedure

This procedure is applicable to all HP.

ILO is an independent subsystem inside a HP server, which is used for out of band remote access. This subsystem permits to monitor, power-off, and power-on the server through a LAN-HTTP interface. The setup of this device shows up during each power-on sequence of the server. When the message for ILO configuration is proposed, hit the <F8> key and follow the on-screen instruction. In case of no user action after a few seconds, the boot sequence continues to the next step. In this situation, it would be necessary to reboot the device to return to this choice.

Recommended configuration consists of assigning an IP address to the system and creates a “root” user. This setup needs to be done in accordance with the customer’s supervision environment.

Minimal steps are:

- Menu “Network”, “DNS/DHCP”, “DHCP enable”, change to OFF, save [F10]
- Menu “Network”, “NIC and TCP/IP”, fill-in the IP address, Subnet Mask, Gateway, Save [F10]
- Menu “User”, “Add user”, “User name” root, “Password”, < same-value-than-TPD >
- Menu “ File”, exit and save

For verification of the setup, connect the ILO interface to the network switch.

1. Open Internet Explorer on a workstation and enter in the ILO IP address.
2. You will get a SSL security warning
3. Accept the warning.
4. Once you are logged in click on Launch to start Integrated Remote Console
5. If you will receive another certificate warning click on Yes to continue
6. If you get the application’s digital signature can not be verified click Always trust content from this publisher then click Run.
7. A remote console window will now appear to allow you to access the HP server.

Granting and revoking DBA role to NSP user

Revoke DBA role from NSP user after NSP installed on one box

1. Login to NSP machine and change user to oracle by command:

```
# su - oracle
```

2. Login to sqlplus console using command:

```
# export ORACLE_SID=NSP

# ORAENV_ASK=NO source oraenv

# sqlplus / as sysdba
```

3. Execute command to revoke DBA and grant necessary privilege from NSP user

```
# REVOKE DBA FROM NSP;

# GRANT CREATE ANY DIRECTORY TO NSP;

# GRANT UNLIMITED TABLESPACE TO NSP;

# GRANT CREATE DATABASE LINK TO NSP;

# GRANT CREATE ANY VIEW TO NSP;
```

Note: Ignore errors if any.

4. Execute below command to confirm that DBA role has been revoked from NSP user or not

```
# SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'NSP';

GRANTED_ROLE

------------

RESOURCE

CONNECT
```

If the result of above command still contains DBA role in result set then **refer to** Appendix A: My Oracle Support

Grant DBA role to NSP user after NSP is installed on one box

1. Login to NSP machine and change user to oracle by command:

```
# su - oracle
```

2. Login to sqlplus console using command:

```
# export ORACLE_SID=NSP

# ORAENV_ASK=NO source oraenv

# sqlplus / as sysdba
```

3. Check whether NSP has DBA role or not by executing below command:

```
# SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'NSP';

GRANTED_ROLE

------------

RESOURCE

CONNECT
```

If the output of command is same as show above then execute below steps to grant DBA role to NSP user but if DBA role is shown in the above list then skip the execution of below steps.

4. Execute command to grant the DBA privilege to NSP user

```
# GRANT DBA TO NSP;
```

Below message will appear on the console after successful completion of the command.

```
Grant succeeded.
```

5. Execute below command to confirm that DBA role has been granted to NSP user or not

```
# SELECT GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'NSP';

GRANTED_ROLE

---------------

RESOURCE

CONNECT

DBA
```

If the result of above command is not the same as shown above and still does not show DBA role in the result set then **refer to** [Appendix A: My Oracle Support]

Modification of the user Profile in Database

Note: The section is applicable for the NSP database user also. The care must be taken to replace the correct NSP user name and profile name (set during the database user creation) in the commands that are going to be executed for Profile modification.

The XDR_PROFILE will be attached with the IXP user with every DTO package upgrade. If the user choose to not to attach the XDR_PROFILE with the user then after the DTO package upgrade, the IXP user should be set with the defaule profile. The XDR_PROFILE is created to provide database related password security. The password policy is attached to the XDR_PROFILE and this can be disabled in the profile if the user does not want any complex password policy.

Swtich IXP user to default profile

1. Login to DWS server and connect to the database as sysdba user:

```
# su – oracle

# sqlplus / as sysdba
```

2. To switch the user to use default profile provided by oracle

```
# SQL> ALTER USER IXP PROFILE default;
# SQL> quit
```

Swtich IXP user to custom profile “XDR_PROFILE”

In case user choose to apply the custom profile XDR_PROFILE to the IXP database user the following commands can be used. The XDR_PROFILE consists of the following parameters:

SESSIONS_PER_USER	UNLIMITED
CPU_PER_SESSION	UNLIMITED
CPU_PER_CALL	UNLIMITED

CONNECT_TIME	UNLIMITED
LOGICAL_READS_PER_SESSION	UNLIMITED
LOGICAL_READS_PER_CALL	UNLIMITED
PRIVATE_SGA	UNLIMITED
COMPOSITE_LIMIT	UNLIMITED
FAILED_LOGIN_ATTEMPTS	5
PASSWORD_LIFE_TIME	UNLIMITED
PASSWORD_REUSE_TIME	UNLIMITED
PASSWORD_REUSE_MAX	20
IDLE_TIME	UNLIMITED
PASSWORD_VERIFY_FUNCTION	ocpic_verify_function
PASSWORD_LOCK_TIME	1
PASSWORD_GRACE_TIME	5
INACTIVE_ACCOUNT_TIME	UNLIMITED'

1. Login to DWS server and connect to the database as sysdba user:

```
# su – oracle

# sqlplus / as sysdba
```

2. To switch the user to use custom XDR_PROFILE

```
# SQL> ALTER USER IXP PROFILE XDR_PROFILE;
# SQL> quit
```

Disable password verification in custom “XDR_PROFILE”

1. Login to DWS server and connect to the database as sysdba user:

```
# su – oracle

# sqlplus / as sysdba
```

2. To disable the password verification in the custom XDR_PROFILE

```
# SQL> ALTER PROFILE XDR_PROFILE LIMIT PASSWORD_VERIFY_FUNCTION NULL;
# SQL> quit
```

Enable password verification in custom "XDR_PROFILE"

1. Login to DWS server and connect to the database as sysdba user:

```
# su – oracle

# sqlplus / as sysdba
```

2. To disable the password verification in the custom XDR_PROFILE

```
# SQL> ALTER PROFILE XDR_PROFILE LIMIT PASSWORD_VERIFY_FUNCTION ocpic_verify_function;
# SQL> quit
```

12. 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.