Corporate Headquarters
5200 Paramount Parkway
Morrisville, NC 27560 USA

GPS

Disaster Recovery Guide

DSR 3.0 and DSR 4.x 2-tier Disaster Recovery

CAUTION

Contact the Tekelec Customer Care Center and inform them of your plans prior to beginning this procedure.

Phone: 1-888-FOR-TKLC (1-888-367-8552) or 919-460-2150 (international)

FAX: 919-460-2126

EMAIL: support@tekelec.com

TABLE OF CONTENTS

List of Tables

List of Procedures

1 INTRODUCTION

1.1 Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for DSR 3.0. This includes recovery of partial or a complete loss of one or more DSR 3.0 servers. The audience for this document includes GPS groups: Software Engineering, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. This document can also be executed by Tekelec customers, as long as Tekelec Customer Service personnel are involved and/or consulted. This document provides step-by-step instructions to execute disaster recovery for DSR 3.0. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note that components dependant on DSR might need to be recovered as well, for example SDS or DIH. To recover those components, refer to the corresponding Disaster Recovery documentation. ([8] for SDS and [9] chapter 6 for DIH)

1.2 References

[1] *HP Solutions Firmware Upgrade Pack Release Notes,* 909-1927-001*,* revision E or latest

[2] *DSR 3.0 on HP C-Class Networking Interconnect Technical Reference*, TR006999, v. 1.6 or greater, P. Mouallem, 2012

[3] *TPD Initial Product Manufacture*, 909-2130-001, v. 1.0 or greater, D. Knierim, 2011

[4] *Platform 6.x Configuration Procedure Reference*, 909-2209-001, v. 1.0 or greater, L. Antosova et al., 2013

[5] *DSR 3.0 HP C-class Installation*, 909-2181-001, latest version, P. Mouallem, 2010

[6] *PM&C 5.x Disaster Recover*, 909-2210-001, latest Version, Tekelec, 2013

[7] *Appworks Database Backup and Restore,* UG005196, latest Version, C. Collard, Jan 2011

[8] *SDS 3.x Disaster Recovery Guide,* TR007061, latest Version, J. Paley, March 2011

[9] *DIH 1.0/1.1 Installation and Upgrade Procedure,* 909-2198-001, latest version, May 2012

[10] *DSR 4.x HP C-class Installation*, 909-2228-001, latest version, P. Mouallem, M. Williams, 2012

[10].3 Software Release Numbering

This procedure applies to all EAGLE XG DSR 3.0 releases.

[10].4 Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DIH	Diameter Intelligent Hub
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MSA	Modular Smart Array
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
PM&C	Platform Management & Configuration
SAN	Storage Area Network
SDS	Subscriber Data Server
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VSP	Virtual Serial Port

[10].5 Terminology

Table 1. Terminology

Base hardware	Base hardware includes all hardware components (bare metal) and electrical wiring to allow a server to power on.
Base software	Base software includes installing the server’s operating system: Tekelec Platform Distribution (TPD).

Failed server	A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.

2 GENERAL DESCRIPTION

The EAGLE XG DSR 3.0 disaster recovery procedure falls into three basic categories. It is primarily dependent on the state of the Network OAM servers:

- Recovery of the entire network from a total outage
    - Both NO servers failed
- Recovery of one or more servers with at least one NO server intact
    - 1 or both NO servers intact
    - 1 or more MP servers failed (This includes IPFE and SBR blades)

Note that for Disaster Recovery of the PM&C Server, Aggregation switches, OA or 6120/3020 switches, refer to Appendix B.

2.1 Complete Server Outage (All servers)

This is the worst case scenario where all the servers in the network have suffered partial or complete software and/or hardware failure. The servers are recovered using base recovery of hardware and software and then restoring a database backup to the active NO server. Database backups will be taken from customer offsite backup storage locations (assuming these were performed and stored offsite prior to the outage). If no backup file is available, the only option is to rebuild the entire network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually.

2.2 Partial Server Outage with NO Server Intact

The simplest case of disaster recovery is with one or both NO servers intact. All servers are recovered using base recovery of hardware and software. Database replication from the active NO server will recover the database to all servers.

3 PROCEDURE OVERVIEW

This section lists the materials required to perform disaster recovery procedures and a general overview (disaster recovery strategy) of the procedure executed.

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document (UG006166) and hardcopies of all documents in the reference list: [1] through [4].
2. Hardcopy of all site surveys performed at the initial installation and network configuration of this customer's site. These can be located in "Q:\custserv" . If the site surveys cannot be found, escalate this issue within Tekelec Customer Service until the site survey documents can be located.
3. EAGLE XG DSR 3.0 database backup file: electronic backup file (preferred) or hardcopy of all EAGLE XG DSR 3.0 configuration and provisioning data. Check [7] for more details on the backup procedure.
4. Latest Network Element report: electronic file or hardcopy of Network Element report.
5. Tekelec Platform Distribution (TPD) Media (32 bits & 64 bits)*.
6. Platform Management & Configuration (PM&C) CD-ROM.
7. EAGLE XG DSR 3.0 CD-ROM (or ISO image file on USB Flash) of the target release.
8. The xml configuration files used to configure the switches, available on the PM&C Server.
9. The network element XML file used for the blades initial configuration.
10. The HP firmware upgrade Kit
11. NetBackup Files if they exist

* The 32-bits TPD is used to IPM the PM&C Server, and the 64-bits TPD is used to IPM the application blades.

11.2 Disaster Recovery Strategy

Disaster recovery procedure execution is performed as part of a disaster recovery strategy with the basic steps listed below:

1. Evaluate failure conditions in the network and determine that normal operations cannot continue without disaster recovery procedures. This means the failure conditions in the network match one of the failure scenarios described in Section 2.
2. Read and review the content in this document.
3. Gather required materials in Section 3.1.
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Table 2).
5. Execute appropriate recovery procedures (listed in Table 2). However be mindful of any other application co-residing with DSR (e.g. SDS), and perform their DR according to the corresponding DR documents.

4 PROCEDURE PREPARATION

Disaster recovery procedure execution is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. Use Table 2 below to evaluate the correct recovery scenario and follow the procedure(s) listed to restore operations.

Note: A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.

Table 2. Recovery Scenarios

Recovery Scenario	Failure Conditions	Procedure
1	• Both NO servers failed. • MP servers may or may not have failed (This includes IPFE and SBR blades).	Execute Section 5.1.1, Procedure 1.
2	• At least 1 NO server is intact and available. • MP servers may or may not have failed (This includes IPFE and SBR blades).	Execute Section 5.1.2, Procedure 2.

5 DISASTER RECOVERY PROCEDURE

Call the Tekelec Customer Care Center at 1-888-FOR-TKLC (1-888-367-8552); or 1-919-460-2150 (international) prior to executing this procedure to ensure that the proper recovery planning is performed.

Before disaster recovery, users must properly evaluate the outage scenario. This check ensures that the correct procedures are executed for the recovery.

****** WARNING *******

****** WARNING *******

NOTE: **DISASTER Recovery is an exercise that requires collaboration of multiple groups and is expected to be coordinated by the TAC prime. Based on TAC's assessment of Disaster, it may be necessary to deviate from the documented process.**

Recovering Base Hardware

1. Hardware Recovery will be executed by Tekelec.
2. Base Hardware Replacement must be controlled by engineer familiar with DSR 4.x Application.

2.1 Recovering and Restoring System Configuration

Disaster recovery requires configuring the system as it was before the disaster and restoration of operational information. There are two distinct procedures to choose from depending on the type of recovery needed. Only one of these should be followed (not both).

2.1.1 Recovery Scenario 1 (Complete Server Outage)

For a complete server outage, NO servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active NO server. All other servers are recovered using recovery procedures of base hardware and software. Database replication from the active NO server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in Procedure 1. The major activities are summarized as follows:

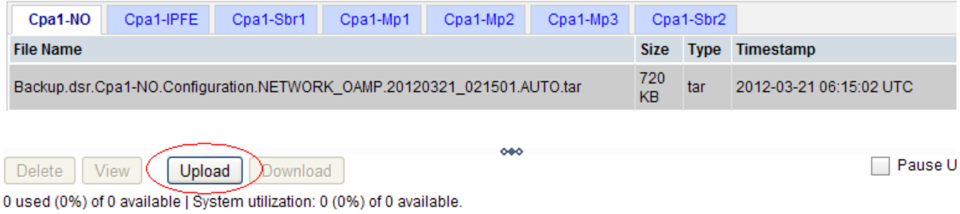
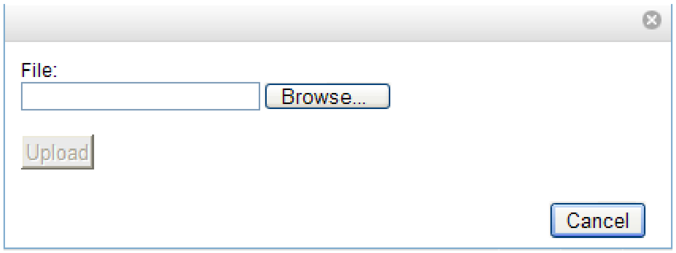
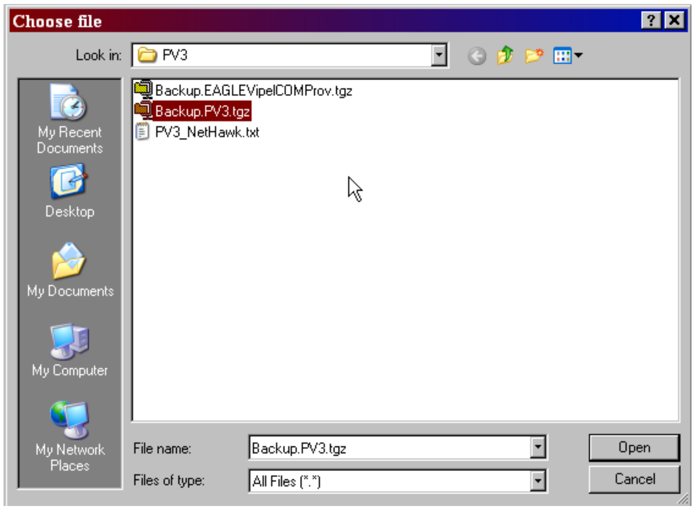
- Recover Base Hardware and Software for all Blades.
    - Recover the base hardware. (by replacing the hardware and executing hardware configuration procedures, reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier).
    - Recover the software. (by executing installation procedures, reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier).
- Recover Active NO server by recovering the database and reconfiguring the application.
    - Recover the database.
    - Reconfigure the application
- Recover Standby NO server by reconfiguring the application
    - Reconfigure the Application
- Recover all MP servers (This includes IPFE and SBR blades) by recovering the application and servers.
    - Reconfigure the application
    - Reconfigure the signaling interfaces and routes on the MPs (by executing installation procedures, reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier).
- Restart processes and re-enable provisioning and replication.

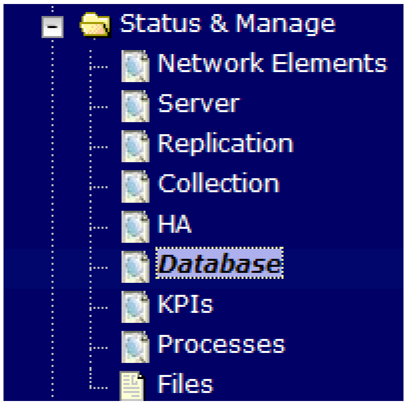
Note that any other applications DR recovery actions (SDS and DIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution (i.e. stale DB on DP servers will not receive updates until SDS-SO servers are recovered

Follow the procedures below for detailed steps.

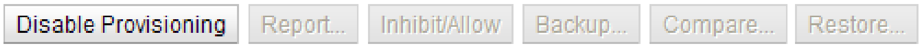
Procedure 1. Recovery Scenario 1

STEP #	This procedure performs recovery if both NO servers have failed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	
1 □	Recover the Failed Hardware and software	Recover the Failed Hardware and Software on ALL failed blades: 1. Gather the documents and required materials listed in Section 3.1. 2. Remove the failed HP c-Class Blades and install the replacement into the enclosure. 3. Configure and verify the BIOS on the Blade. Execute procedure “Confirm/Update Blade Server BIOS Settings” from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 4. Execute Procedure “Configure iLO password for Blades’ Administrator Account” from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier to setup the root password on the newly installed blade. 5. Load any firmware and errata upgrades using [1]. 6.Execute procedure “Install TVOE on VM Host Server Blades” from reference [5] if recovering DSR 3.0 or “Install TVOE on Server Blade” from [10] if recovering DSR 4.x 2-tier. 7.Execute procedure “Configure TVOE on Server Blades” from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 8. instruct any other Application’s personnel to start recovery procedures on the Guests hosted by the server (parallel recovery). 9.Execute procedure “Create NOAMP Guest VMs” from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 10. IPM all the blades using procedure “IPM Blades” from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 11. If recovering a DSR 4.x 2-tier system, ssh to the system as root from the pm&c using the control IP address of the NO (192.168.1.x) and execute the following command (The control IP address can be viewed from the pmac GUI): **touch /usr/TKLC/DsrDataAsourced** 12. Install the application on the all the blades using procedure “Install the Application Software on the Blades” from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. Repeat this step for all remaining failed blades.
2 □	Obtain latest database backup and network configuration data.	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. Determine network configuration data. 1. Using procedures within your organization’s process (ex. IT department recovery procedures), obtain the most recent backup of the EAGLE XG DSR 3.0/4.x database backup file. 2. From required materials list in Section 3.1; use site survey documents and Network Element report (if available), to determine network configuration data.
3 □	Execute EAGLE XG DSR Installation procedures.	Execute procedures from EAGLEXG DSR 3.0/4.x Installation User’s Guide. 1. Verify the networking data for Network Elements. Use the backup copy of network configuration data and site surveys (from Step 2) 2. Install the first NO server, you will need to obtain the network element XML file from the PM&C Server: Execute installation procedures for the first NO server. See reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier, Procedure “Configure the First NOAMP Server”, and “Configure the NOAMP Server Group”.
4 □	Login into the NO XMI VIP Address of	Log into the first NO GUI.

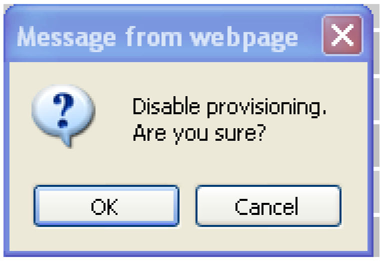
5 □	Upload the backed up database file from Remote location into File Management Area.	1. Browse to Main Menu->Status & Manage->Files 2. Select the Active NO Server. The following screen will appear. Click on "Upload" as shown below and select the file "Provisioning and Configuration:" file backed up after initial installation and provisioning.  Cpa1-NO Cpa1-IPFE Cpa1-Sbr1 Cpa1-Mp1 Cpa1-Mp2 Cpa1-Mp3 Cpa1-Sbr2 File Name | Size | Type | Timestamp Backup.dsr.Cpa1-NO.Configuration.NETWORK_OAMP.20120321_021501.AUTO.tar | 720 KB | tar | 2012-03-21 06:15:02 UTC 0 used (0%) of 0 available | System utilization: 0 (0%) of 0 available. 3. Click on "Browse" and Locate the backup file and click on "Open" as shown below.   Choose file Look in: PV3 My Recent Documents Desktop My Documents My Computer My Network Places Open Cancel Backup.EAGLEVipelCOMProv.tgz Backup.PV3.tgz PV3_NetHawk.txt File name: Backup.PV3.tgz Files of type: All Files (*.*) 4. Click on the "Upload " button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
6 □	Disable Provisioning	1. Click on Main Menu->Status & Manage->Database



2. Disable Provisioning by clicking on “Disable Provisioning” button at the bottom of the screen as shown below.



3. A confirmation window will appear, press “OK” to disable Provisioning.

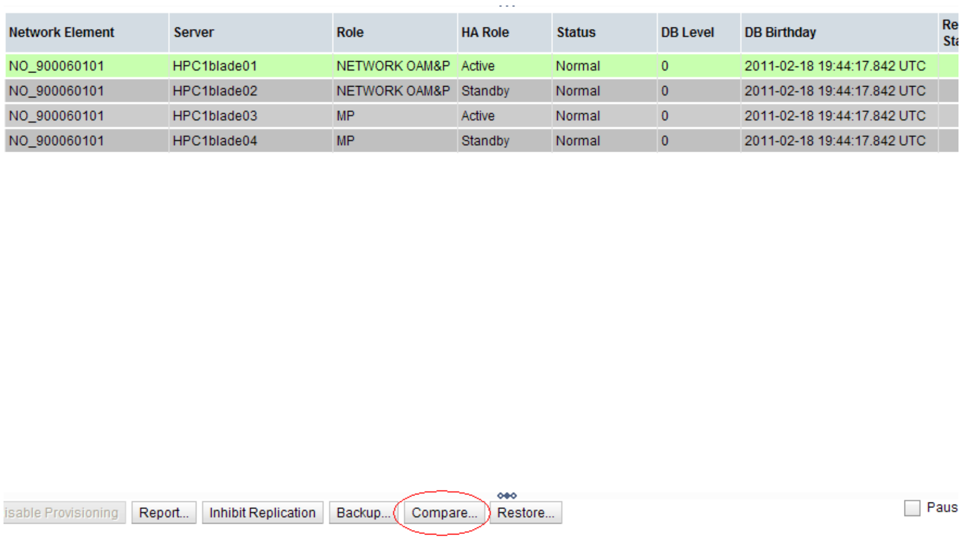


Disable provisioning.
Are you sure?

4. The message “Warning Code 002” will appear.

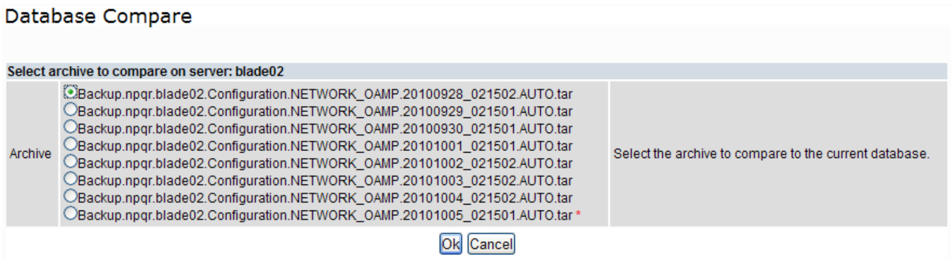
7 □ Verify the Archive Contents and Database Compatibility

1. Select the Active NO Server and click on the “Compare”:



Network Element	Server	Role	HA Role	Status	DB Level	DB Birthday	Re Sta
NO_900060101	HPC1blade01	NETWORK OAM&P	Active	Normal	0	2011-02-18 19:44:17.842 UTC	
NO_900060101	HPC1blade02	NETWORK OAM&P	Standby	Normal	0	2011-02-18 19:44:17.842 UTC	
NO_900060101	HPC1blade03	MP	Active	Normal	0	2011-02-18 19:44:17.842 UTC	
NO_900060101	HPC1blade04	MP	Standby	Normal	0	2011-02-18 19:44:17.842 UTC	

2. The following screen is displayed; click the radio button for the restored database file that was uploaded as a part of Step 2 of this procedure.

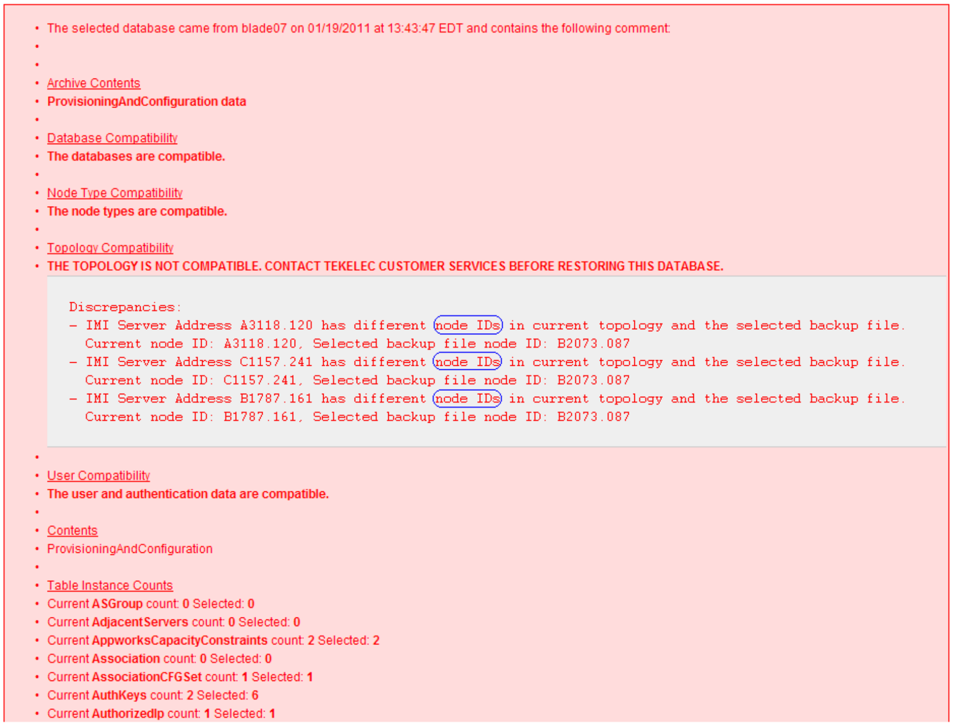


Database Compare

Select archive to compare on server: blade02

Archive	● Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar ○ Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar ○ Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100930_021501.AUTO.tar ○ Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101001_021501.AUTO.tar ○ Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar ○ Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101003_021502.AUTO.tar ○ Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101004_021502.AUTO.tar ○ Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar *	Select the archive to compare to the current database.

3. Verify that the output window matches the screen below. Note that you will get a database mismatch regarding the NodeIDs of the blades. That is expected. If that is the only mismatch, then you can proceed, otherwise stop and contact customer support



- The selected database came from blade07 on 01/19/2011 at 13:43:47 EDT and contains the following comment:
-
-
- Archive Contents
- **ProvisioningAndConfiguration data**
-
- Database Compatibility
- **The databases are compatible.**
-
- Node Type Compatibility
- **The node types are compatible.**
-
- Topology Compatibility
- **THE TOPOLOGY IS NOT COMPATIBLE. CONTACT TEKELEC CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.**

```
Discrepancies:
- IMI Server Address A3118.120 has different node IDs in current topology and the selected backup file.
  Current node ID: A3118.120, Selected backup file node ID: B2073.087
- IMI Server Address C1157.241 has different node IDs in current topology and the selected backup file.
  Current node ID: C1157.241, Selected backup file node ID: B2073.087
- IMI Server Address B1787.161 has different node IDs in current topology and the selected backup file.
  Current node ID: B1787.161, Selected backup file node ID: B2073.087
```

-
- User Compatibility
- **The user and authentication data are compatible.**
-
- Contents
- ProvisioningAndConfiguration
-
- Table Instance Counts
- Current **ASGroup** count: **0** Selected: **0**
- Current **AdjacentServers** count: **0** Selected: **0**
- Current **AppworksCapacityConstraints** count: **2** Selected: **2**
- Current **Association** count: **0** Selected: **0**
- Current **AssociationCFGSet** count: **1** Selected: **1**
- Current **AuthKeys** count: **2** Selected: **6**
- Current **AuthorizedIp** count: **1** Selected: **1**

NOTE: Archive Contents and Database Compatibilities must be the following:

Archive Contents: Configuration data

Database Compatibility: The databases are compatible.

NOTE: Following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one NOAMP:

Topology Compatibility
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

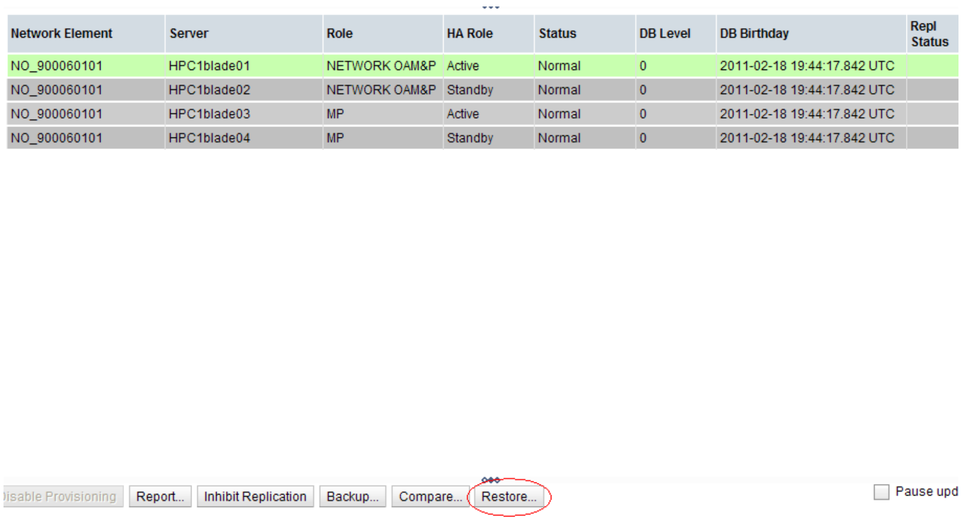
NOTE: We are trying to restore a backed up database onto an empty NOAMP database. This is an expected text in Topology Compatibility.

4. If the verification is successful, Click BACK button and continue to next step in this procedure.

8 Restore the Database

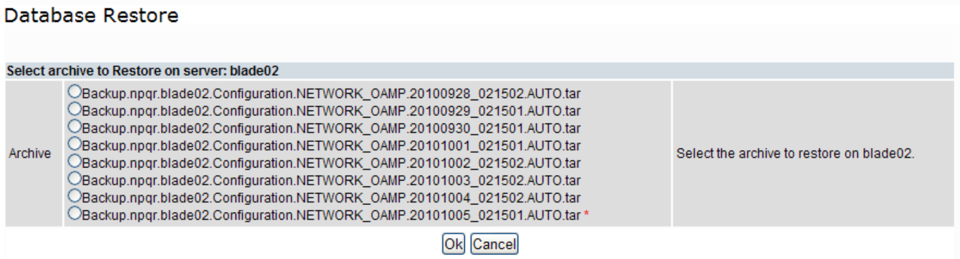
☐

1. Click on Main Menu->Status & Manage->Database
2. Select the Active NO Server, and click on “Restore” as shown below.



Network Element	Server	Role	HA Role	Status	DB Level	DB Birthday	Repl Status
NO_900060101	HPC1blade01	NETWORK OAM&P	Active	Normal	0	2011-02-18 19:44:17.842 UTC	
NO_900060101	HPC1blade02	NETWORK OAM&P	Standby	Normal	0	2011-02-18 19:44:17.842 UTC	
NO_900060101	HPC1blade03	MP	Active	Normal	0	2011-02-18 19:44:17.842 UTC	
NO_900060101	HPC1blade04	MP	Standby	Normal	0	2011-02-18 19:44:17.842 UTC	

3. The following screen will be displayed. Select the proper back up provisioning and configuration file.



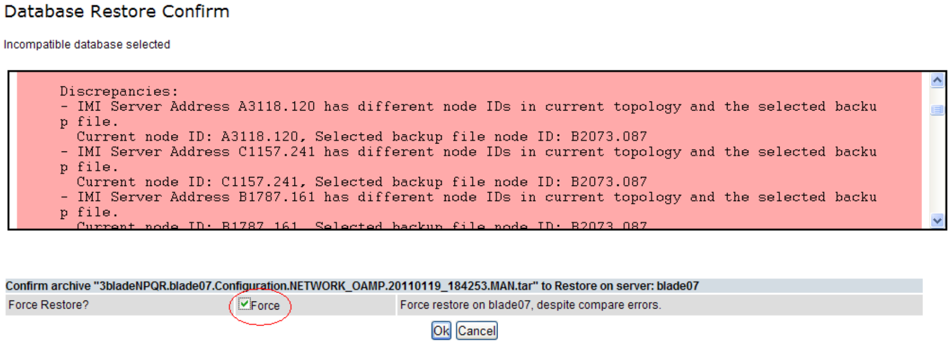
Database Restore

Select archive to Restore on server: blade02

Archive	○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100930_021501.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101001_021501.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101003_021502.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101004_021502.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar *	Select the archive to restore on blade02.

4. Click “OK” Button. The following confirmation screen will be displayed.

5. If you get an error that the NodeIDs do not match. That is expected. If no other errors beside the NodeIDs are displayed, select the “Force” checkbox as shown above and Click OK to proceed with the DB restore.



Database Restore Confirm

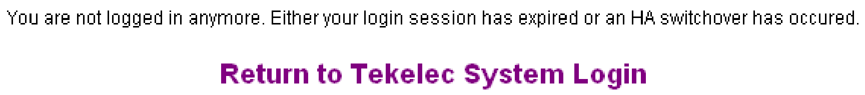
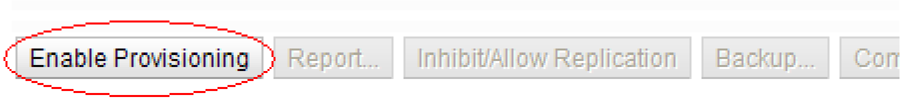
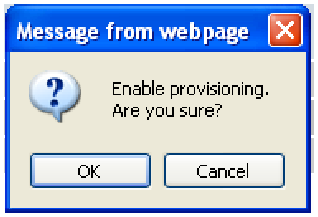
Incompatible database selected

```
Discrepancies:
- IMI Server Address A3118.120 has different node IDs in current topology and the selected backu
p file.
  Current node ID: A3118.120, Selected backup file node ID: B2073.087
- IMI Server Address C1157.241 has different node IDs in current topology and the selected backu
p file.
  Current node ID: C1157.241, Selected backup file node ID: B2073.087
- IMI Server Address B1787.161 has different node IDs in current topology and the selected backu
p file.
  Current node ID: B1787.161, Selected backup file node ID: B2073.087
```

Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07

Force Restore?	☑Force	Force restore on blade07, despite compare errors.

6. **NOTE:** After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data. The following logout screen is displayed automatically

		 You are not logged in anymore. Either your login session has expired or an HA switchover has occured. **Return to Tekelec System Login** 7. Log in Back into GUI VIP by clicking “Continue to this Website” 8. Login using the guiadmin login and password into the GUI 9. Wait for 5-10 minutes for the System to stabilize with the new topology. 10. Following Alarms must be ignored for NO and MP Servers until all the Servers are configured. Alarms with Type Column as “REPL” , “COLL”, “HA” (with mate NOAMP), “DB” (about Provisioning Manually Disabled) ***Do not pay attention to alarms until all the servers in the system are completely restored.*** ***NOTE: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.***
9 □	Re-enable Provisioning	1. Click on Main Menu->Status & Manage->Database menu item.  Enable Provisioning Report... Inhibit/Allow Replication Backup... Con 2. Click on the “Enable Provisioning” button. A pop-up window will appear to confirm as shown below, press OK. Message from webpage Enable provisioning. Are you sure?
10 □	Recover standby NO server.	Recover the standby NO server: 1. Install the second NO server by executing the following procedure from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier: “Configure the Second NOAMP Server, steps 1, 4, 5 and 6”.
11 □	Recover the MP Servers (also applies to IPFE servers)	Execute the following procedures from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier FOR **EACH** MP that has been recovered: 1.”Configure MP Blades Servers”, Steps 1, 4, 5, 6 and 7 2. Reapply the signaling Networking Configuration by running the following command from the active NO command line for each MP Server: **/usr/TKLC/appworks/bin/syncApplConfig <MP_Hostame>**
12 □	Restart Application Processes	Restart the Application by Navigating to **Status & Manage** -> **Server,** then select each server that has been recovered and clicking on **Restart** at the bottom of the screen.

13 □ Allow Replication to all Servers

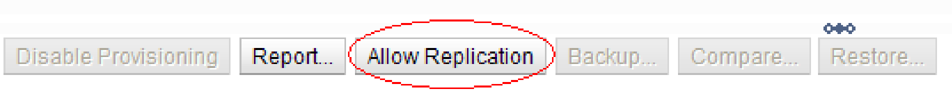
1. Navigate to Status & Manage -> Database
2. If the “Repl Status” is set to “Inhibited”, click on the “Allow Replication” button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step.:

   a. Active NOAMP Server

   b. Standby NOAMP Server

   c. Active MP Servers

   d. Standby MP Servers



Verify that the replication on all servers is allowed. This can be done by clicking on each server and checking that the button below shows “Inhibit” Replication” instead of “Allow Replication”.

14 □ Remove Forced Standby

If recovering a DSR 3.0 system, execute:

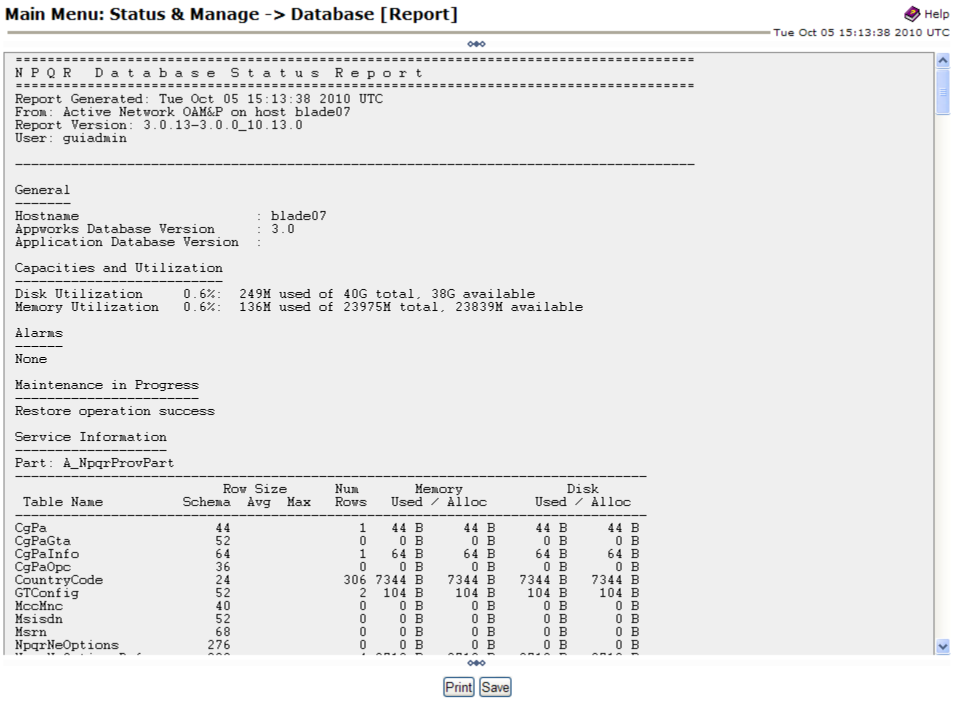
1. Navigate to Status & Manage -> HA
2. For each server which it’s HA Status is in “Forced Standby”, Select that server and click on the “Disable Forced Standby” button located at the bottom of the screen. Starting with the NOs then MPs. If no servers are in “Forced Standby” then skip this step.
3. Repeat this step for every server in the “Forced Standby” state.

If recovering a DSR 4.x 2-tier system, then execute:

1. Navigate to Status & Manage -> HA
2. Click on **Edit** at the bottom of the screen
3. For each server whose **Max Allowed HA Role is** set to Standby, set it to Active
4. Press **OK**

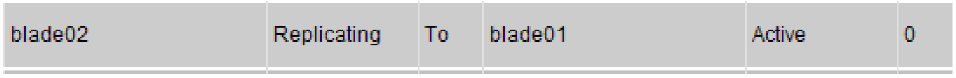
15 □ Fetch and Store the database Report for the newly restored data and save it

1. Navigate to Configuration-> Server, select the active NO server and click on the “Report” button at the bottom of the page . The following screen is displayed:


Main Menu: Status & Manage -> Database [Report]
Help
Tue Oct 05 15:13:38 2010 UTC
Print
Save

```
=====================================================================================
N P Q R   D a t a b a s e   S t a t u s   R e p o r t
=====================================================================================
Report Generated: Tue Oct 05 15:13:38 2010 UTC
From: Active Network OAM&P on host blade07
Report Version: 3.0.13-3.0.0_10.13.0
User: guiadmin

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

General
-------
Hostname                        : blade07
Appworks Database Version       : 3.0
Application Database Version    :

Capacities and Utilization
--------------------------
Disk Utilization      0.6%:  249M used of 40G total, 38G available
Memory Utilization    0.6%:  136M used of 23975M total, 23839M available

Alarms
------
None

Maintenance in Progress
-----------------------
Restore operation success

Service Information
-------------------
Part: A_NpqrProvPart
-------------------------------------------------------------------------------
                        Row Size        Num        Memory            Disk
 Table Name          Schema  Avg  Max   Rows    Used / Alloc      Used / Alloc
-------------------------------------------------------------------------------
CgPa                     44                1    44 B      44 B    44 B      44 B
CgPaGta                  52                0     0 B       0 B     0 B       0 B
CgPaInfo                 64                1    64 B      64 B    64 B      64 B
CgPaOpc                  36                0     0 B       0 B     0 B       0 B
CountryCode              24              306  7344 B    7344 B  7344 B    7344 B
GTConfig                 52                2   104 B     104 B   104 B     104 B
MccMnc                   40                0     0 B       0 B     0 B       0 B
Msisdn                   52                0     0 B       0 B     0 B       0 B
Msrn                     68                0     0 B       0 B     0 B       0 B
NpqrNeOptions           276                0     0 B       0 B     0 B       0 B
```

2. Click on “Save” and save the report to your local machine.

17 □	Verify Replication between servers.	If restoring a DSR 3.0 system, Navigate to Main Menu->Status and Manage->Replication and Verify that replication is occurring between servers as shown below.  blade02 Replicating To blade01 Active 0 If restoring a DSR 4.x 2-tier system, Navigate to Main Menu->Status and Manage -> Database and verify that replication is occurring between servers.
18 □	Verify the HA states	1. Click on Main Menu->Status and Manager->Database 2. Verify that the HA Role (or OAM Max HA Role for DSR 4.x) is either “Active” or “Standby”.
19 □	Verify the local node info	1. Click on Main Menu->Diameter->Configuration->Local Node 2. Verify that all the local nodes are listed.
20 □	Verify the peer node info	1. Click on Main Menu->Diameter->Configuration->Peer Node 2. Verify that all the peer nodes are listed.
21 □	Verify the Connections info	1. Click on Main Menu->Diameter->Configuration->Connections 2. Verify that all the peer nodes are listed.
23 □	Re-enable connections if needed	1. Click on Main Menu->Diameter->Maintenance->Connections 2. Select each connection and click on the “Enable” button 3. Verify that the Operational State is Available.
24 □	Examine All Alarms	1. Click on Main Menu->Alarms & Events->View Active 2. Examine all active alarms and refer to the on-line help on how to address them. If needed contact the Tekelec Customer Support hotline.
25 □	Restore GUI Username s and passwords	If applicable, Execute steps in Section 6 to recover the user and group information restored.
26 □	Re-activate Optional Features	Optional features (such as RBAR, Mediation, etc) might need to be deactivated and re-actived for them to operate properly. Refer to [10] for more details on how to do so.
27 □	Backup and archive all the databases from the recovered system	Execute Appendix A back up the Configuration databases: Disaster Recovery Procedure is Complete

End of Procedure

2.d..2

Recovery Scenario 2 (Partial Server Outage with NO Server Intact)

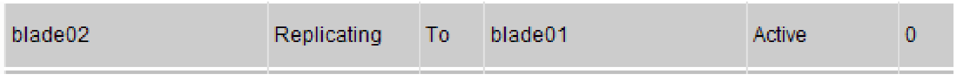
For a partial outage with an NO server intact and available, only base recovery of hardware and software is needed. The single NO server is capable of restoring the database via replication to all servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in Procedure 2. The major activities are summarized as follows:

- Recover Standby NO server (if necessary) by recovering base hardware and software.
  - **Recover** the base **hardware**.
  - **Recover** the **software**.
  - The database is intact at the active NO server and does not require restoration at the standby NO server.
- Recover any failed MP(s) servers by recovering base hardware and software.
  - **Recover** the base **hardware**.
  - **Recover** the **software**.
  - The database has already been restored at the active NO server and does not require restoration at the SO and MP servers.

Follow the procedure below for detailed steps.

Procedure 2. Recovery Scenario 2

S T E P #	This procedure performs recovery if at least 1 NO servers intact and available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	
1 □	Recover standby NO server (if needed).	Recover the standby NO server (if needed) by recovering base hardware and software. If both NO servers are intact and available, skip this step and go to Step 2. If the standby NO server has failed: 1. Gather the documents and required materials listed in Section 3.1. These are the same documents which were required in Step 2. 2. From the NO VIP GUI, Inhibit replication to the standby NO by navigating to Main Menu->Status & Manage-> Database, then selecting the NO in question and clicking on “Inhibit Replication”. 3. From the NO VIP GUI, set the server HA state to “Forced Standby” by navigating to Main Menu->HA and : • If recovering a DSR 3.0 system: Select the NO in question and checking the “Enabled” checkbox next to Forced Standby and pressing OK. • If recovering a DSR 4.0 2-tier system: Click on Edit and setting the “Max Allowed HA Role” to Standby for the NO in question and pressing OK. 4. Remove the failed HP c-Class Blade and install the replacement into the enclosure. 5. Configure and verify the BIOS on the Blade. Execute procedure “Confirm/Update Blade Server BIOS Settings” from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier.. 6. Execute Procedure “Configure iLO password for Blades’ Administrator Account” from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier to setup the root password on the newly installed blade. 7.Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details. 8.Execute procedure “Install TVOE on VM Host Server Blades” from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 9.Execute procedure “Configure TVOE on Server Blades” from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 10.Execute procedure “Create NOAMP Guest VMs” from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 11. If the blade hosts any other applications (e.g. SDS), instruct any other Application’s personnel to start recovery procedures on the Guests hosted by the server . 12. IPM The standby NO using procedure “IPM Blades” from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 13. f recovering a DSR 4.x 2-tier system, logon to the system’s command line as root and execute the following command: **touch /usr/TKLC/DsrDataAsourced** 14. Install the application on the Standby NO using procedure “Install the Application Software on the Blades” from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 15. Configure the newly installed application by executing procedure “Configure the Second NOAMP Server steps 1, 2, 4, 5 and 6. 16. Re-enable Replication to the restored NO by navigating to Main Menu->Status & Manage-> Database, then selecting the NO in question and clicking on “Allow Replication”. 17. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered server and Clicking on “Restart”.

2 □	Recover MP servers (if needed, also applies to IPFE).	Recover the MP server(s) (if needed) by recovering base hardware and software. Execute the following for any MP server that has failed: 1. From the NO VIP GUI, Inhibit replication to the failed MP(s) by navigating to Main Menu->Status & Manage-> Database, then selecting the MP in question and clicking on “Inhibit Replication”. 2. Remove the failed HP c-Class Blade and install the replacement into the enclosure. 3. Configure and verify the BIOS on the Blade. Execute procedure “Confirm/Update Blade Server BIOS Settings” from reference [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 4. Execute Procedure “Configure iLO password for Blades’ Administrator Account” from [5] to setup the root password on the newly installed blade. 5. IPM The failed MP(s) using procedure “IPM Blades” from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 6. If recovering a DSR 4.x 2-tier system, logon to the system’s command line as root and execute the following command: **touch /usr/TKLC/DsrDataAsourced** 7. Install the application on the failed MP(s) using procedure “Install the Application Software on the Blades” from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 8. Execute the following procedures ”Configure MP Blades Servers”, Steps 1, 2, 4, 5 and 6 from [5] if recovering DSR 3.0 or [10] if recovering DSR 4.x 2-tier. 9. Re-enable Replication to the restored MP(s) by navigating to Main Menu->Status & Manage-> Database, then selecting the MP in question and clicking on “Allow Replication”. 10. Reapply the signaling Networking Configuration by running the following command from the active NO command line: **/usr/TKLC/appworks/bin/syncApplConfig <Recovered_MP_Hostame>** 11. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered servers and Clicking on “Restart”.
3 □	Remove Forced Standby	If recovering a DSR 3.0 system, execute: 4. Navigate to Status & Manage -> HA 5. For each server which it’s HA Status is in “Forced Standby”, Select that server and click on the “Disable Forced Standby” button located at the bottom of the screen. Starting with the NOs then MPs. If no servers are in “Forced Standby” then skip this step. 6. Repeat this step for every server in the “Forced Standby” state. If recovering a DSR 4.x 2-tier system, then execute: 5. Navigate to Status & Manage -> HA 6. Click on **Edit** at the bottom of the screen 7. For each server whose **Max Allowed HA Role is** set to Standby, set it to Active 8. Press **OK**
4 □	Verify Replication between servers.	If restoring a DSR 3.0 system, Navigate to Main Menu->Status and Manage->Replication and Verify that replication is occurring between servers as shown below.  blade02 Replicating To blade01 Active 0 If restoring a DSR 4.x 2-tier system, Navigate to Main Menu->Status and Manage -> Database and verify that replication is occurring between servers.
5 □	Verify the HA states	1. Click on Main Menu->Status and Manager->Database 2. Verify that the HA Role (or OAM Max HA Role for DSR 4.x) is either “Active” or “Standby”.
6 □	Verify the local node info	1. Click on Main Menu->Diameter->Configuration->Local Node 2. Verify that all the local nodes are listed.

7 □	Re-install NetBackup (Optional)	1. If NetBackup was previously installed on the system, follow the procedure in [5], Appendix K to reinstall it.
8 □	Verify the peer node info	1. Click on Main Menu->Diameter->Configuration->Peer Node 2. Verify that all the peer nodes are listed.
9 □	Verify the Connections info	1. Click on Main Menu->Diameter->Configuration->Connections 2. Verify that all the peer nodes are listed.
10 □	Re-enable connections if needed	1. Click on Main Menu->Diameter->Maintenance->Connections 2. Select each connection and click on the “Enable” button 3. Verify that the Operational State is Available.
11 □	Examine All Alarms	1. Click on Main Menu->Alarms & Events->View Active 2. Examine all active alarms and refer to the on-line help on how to address them. If needed contact the Tekelec Customer Support hotline.
12 □	Backup and archive all the databases from the recovered system	Execute Appendix A back up the Configuration databases: Disaster Recovery Procedure is Complete

End of Procedure

6 RESOLVING USER CREDENTIAL ISSUES AFTER DATABASE RESTORE

User incompatibilities may introduce security holes or prevent access to the network by administrators. User incompatibilities are not dangerous to the database, however. Review each user difference carefully to ensure that the restoration will not impact security or accessibility.

6.1 Restoring a Deleted User

```
- User 'testuser' exists in the selected backup file but not in the current
database.
```

These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

6.1.1 To Keep the Restored User

Perform this step to keep users that will be restored by system restoration.

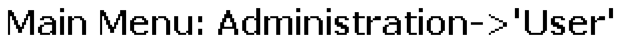
Before restoration,

- Contact each user that is affected and notify them that you will reset their password during this maintenance operation.

After restoration

- Log in and reset the passwords for all users in this category.

1. Navagate to the user administration screen.

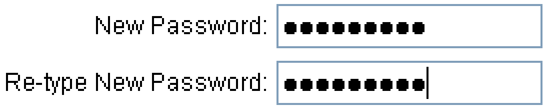


Main Menu: Administration->'User'

2. Select the user.

3. Click the Change Password button.

4. Enter a new password.



New Password: ●●●●●●●●●●

Re-type New Password: ●●●●●●●●●●

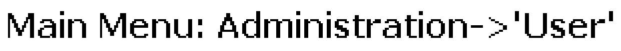
5. Click the Continue button.

5..1.2 To Remove the Restored User

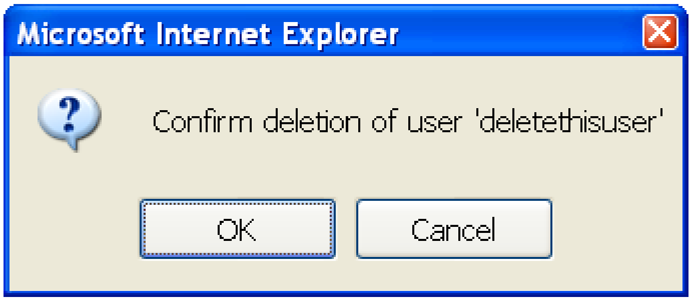
Perform this step to remove users that will be restored by system restoration.

After restoration, delete all users in this category.

1. Navagate to the user administration screen.


Main Menu: Administration->'User'

2. Select the user.
3. Click the Delete button.
4. Confirm.



Confirm deletion of user 'deletethisuser'

4.2 Restoring a Modified User

These users have had a password change prior to creation of the backup and archive file. The will be reverted by system restoration of that file.

```
- The password for user 'testuser' differs between the selected backup file and
the current database.
```

Before restoration,

- Verify that you have access to a user with administrator permissions that is not affected.
- Contact each user that is affected and notify them that you will reset their password during this maintenance operation.

After restoration

- Log in and reset the passwords for all users in this category. See the steps in section 6.1.1 for resetting passwords for a user.

4..3 Restoring an Archive that Does not Contain a Current User

These users have been created after the creation of the backup and archive file. The will be deleted by system restoration of that file.

```
- User 'testuser' exists in current database but not in the selected backup file.
```

If the user is no longer desired, do not perform any additional steps. The user is permanently removed.

To re-create the user, do the following:

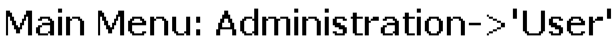
Before restoration,

- Verify that you have access to a user with administrator permissions that is not affected.
- Contact each user that is affected and notify them that you will reset their password during this maintenance operation.
- Log in and record the username, group, timezone, comment, and enabled values for each affected user.

After restoration

- Log in and re-create each of the affected users using the information recorded above

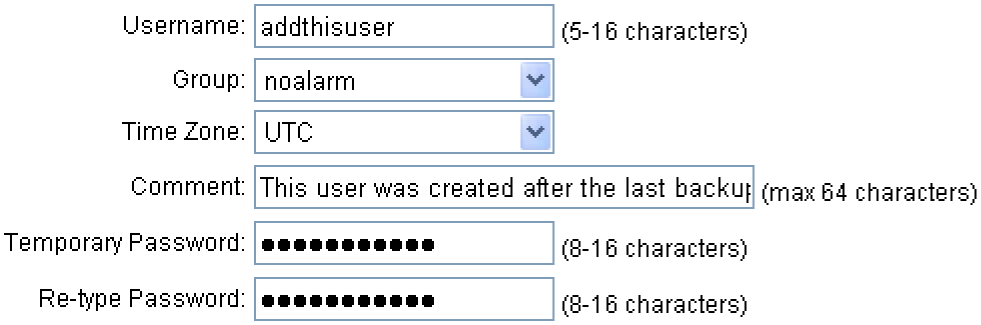
1. Navagate to the user administration screen.



Main Menu: Administration->'User'

2. Click the Add New User button.

3. Re-populate all the data for this user.



Username: addthisuser (5-16 characters)

Group: noalarm

Time Zone: UTC

Comment: This user was created after the last backup (max 64 characters)

Temporary Password: ●●●●●●●●●●●● (8-16 characters)

Re-type Password: ●●●●●●●●●●●● (8-16 characters)

4. Click the OK button.

- Reset the passwords for all users in this category. See the steps in section 6.1.1 for resetting passwords for a user.

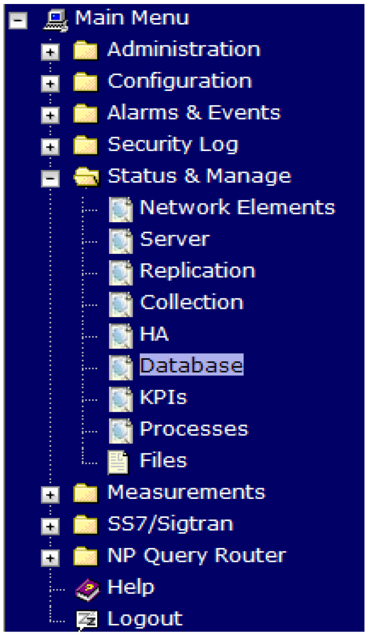
Appendix A. EAGLEXG DSR 3.0 Database Backup

Procedure 3: DSR 3.0 / 4.x 2-tier Database Backup

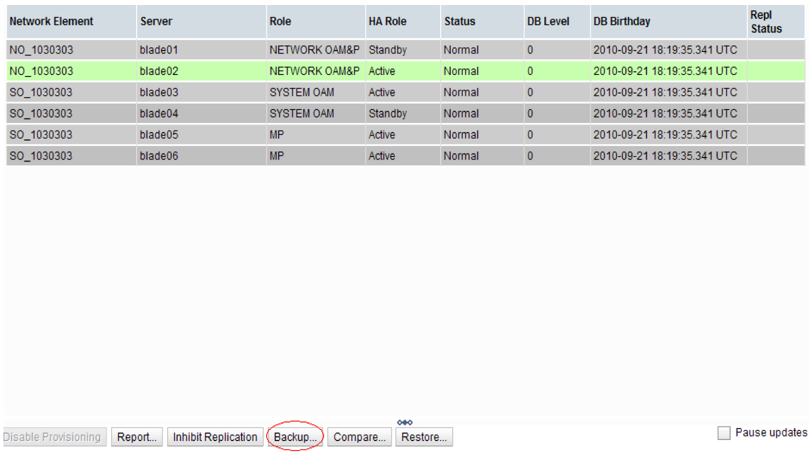
<table>
<tr><th>S
T
E
P
#</th><td colspan="2">The intent of this procedure is to backup the provision and configuration information after the disaster recovery is complete and transfer it to a secure location accessible to TAC.
Prerequisites for this procedure are:
• Network connectivity to the NO XMI address via VPN access to the Customer's network.
• DSR 3.0 /4.x 2-tier "guiadmin" user password.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.</td></tr>
<tr><td>1.</td><td><b>Login into NO XMI VIP IP Address</b></td><td>Login using the "guiadmin" credentials.</td></tr>
</table>

2. **Backup provisioning and Configuration data for the system.**

1. Browse to Main Menu->Status & Manage->Database screen

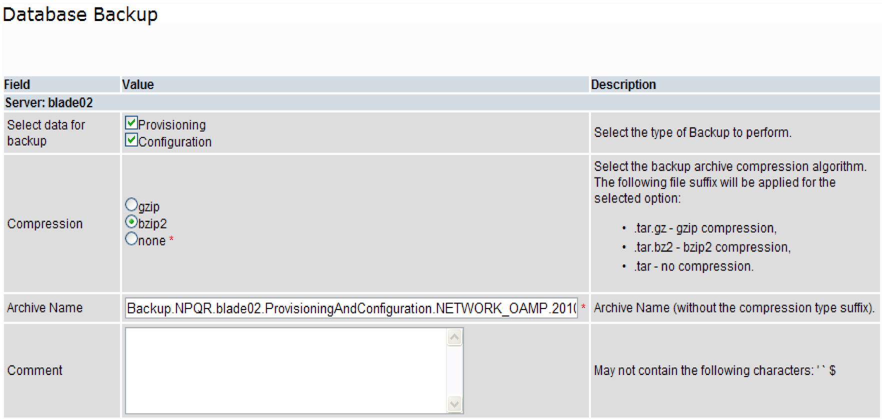


2. Select the Active NOAMP Server and Click on “Backup” button as shown :



Network Element	Server	Role	HA Role	Status	DB Level	DB Birthday	Repl Status
NO_1030303	blade01	NETWORK OAM&P	Standby	Normal	0	2010-09-21 18:19:35.341 UTC	
NO_1030303	blade02	NETWORK OAM&P	Active	Normal	0	2010-09-21 18:19:35.341 UTC	
SO_1030303	blade03	SYSTEM OAM	Active	Normal	0	2010-09-21 18:19:35.341 UTC	
SO_1030303	blade04	SYSTEM OAM	Standby	Normal	0	2010-09-21 18:19:35.341 UTC	
SO_1030303	blade05	MP	Active	Normal	0	2010-09-21 18:19:35.341 UTC	
SO_1030303	blade06	MP	Active	Normal	0	2010-09-21 18:19:35.341 UTC	

3. Make sure that the checkboxes next to Configuration and Provisioning (if selectable) are both checked. Then enter a filename for the backup and press “OK”._

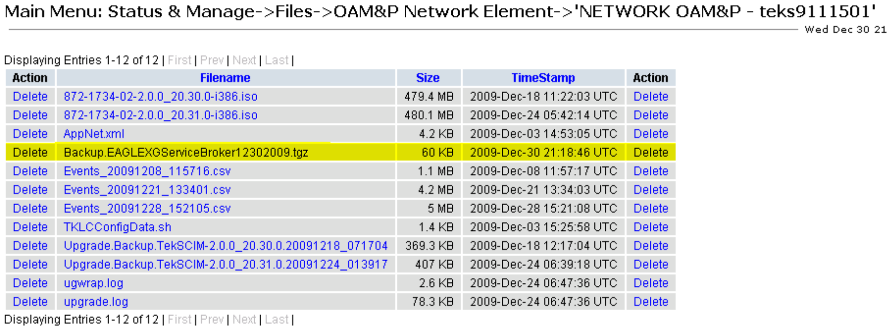


Database Backup

Field	Value	Description
Server: blade02		
Select data for backup	☑ Provisioning ☑ Configuration	Select the type of Backup to perform.
Compression	○ gzip ● bzip2 ○ none *	Select the backup archive compression algorithm. The following file suffix will be applied for the selected option: • .tar.gz - gzip compression, • .tar.bz2 - bzip2 compression, • .tar - no compression.
Archive Name	Backup.NPQR.blade02.ProvisioningAndConfiguration.NETWORK_OAMP.201(*	Archive Name (without the compression type suffix).
Comment		May not contain the following characters: ' ` $

3. **Verify the back up file availability.**

1. Browse to Main Menu-> Status & Manage->Files
2. Select the Active NO and click on “List Files”
3. The files on this server file management area will be displayed in the work area.



Main Menu: Status & Manage->Files->OAM&P Network Element->'NETWORK OAM&P - teks9111501'

Wed Dec 30 21

Displaying Entries 1-12 of 12 | First | Prev | Next | Last |

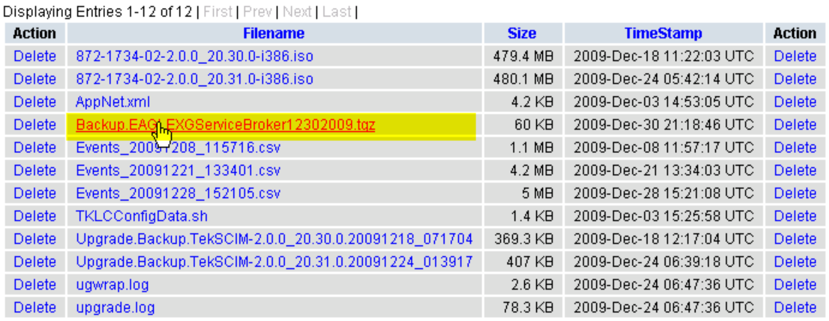
Action	Filename	Size	TimeStamp	Action
Delete	872-1734-02-2.0.0_20.30.0-i386.iso	479.4 MB	2009-Dec-18 11:22:03 UTC	Delete
Delete	872-1734-02-2.0.0_20.31.0-i386.iso	480.1 MB	2009-Dec-24 05:42:14 UTC	Delete
Delete	AppNet.xml	4.2 KB	2009-Dec-03 14:53:05 UTC	Delete
Delete	Backup.EAGLEXGServiceBroker12302009.tgz	60 KB	2009-Dec-30 21:18:46 UTC	Delete
Delete	Events_20091208_115716.csv	1.1 MB	2009-Dec-08 11:57:17 UTC	Delete
Delete	Events_20091221_133401.csv	4.2 MB	2009-Dec-21 13:34:03 UTC	Delete
Delete	Events_20091228_152105.csv	5 MB	2009-Dec-28 15:21:08 UTC	Delete
Delete	TKLCConfigData.sh	1.4 KB	2009-Dec-03 15:25:58 UTC	Delete
Delete	Upgrade.Backup.TekSCIM-2.0.0_20.30.0.20091218_071704	369.3 KB	2009-Dec-18 12:17:04 UTC	Delete
Delete	Upgrade.Backup.TekSCIM-2.0.0_20.31.0.20091224_013917	407 KB	2009-Dec-24 06:39:18 UTC	Delete
Delete	ugwrap.log	2.6 KB	2009-Dec-24 06:47:36 UTC	Delete
Delete	upgrade.log	78.3 KB	2009-Dec-24 06:47:36 UTC	Delete

Displaying Entries 1-12 of 12 | First | Prev | Next | Last |

4. Verify the existence of the backed up provisioning & configuration back up file as shown above.

4. **Download the file to local machine.**

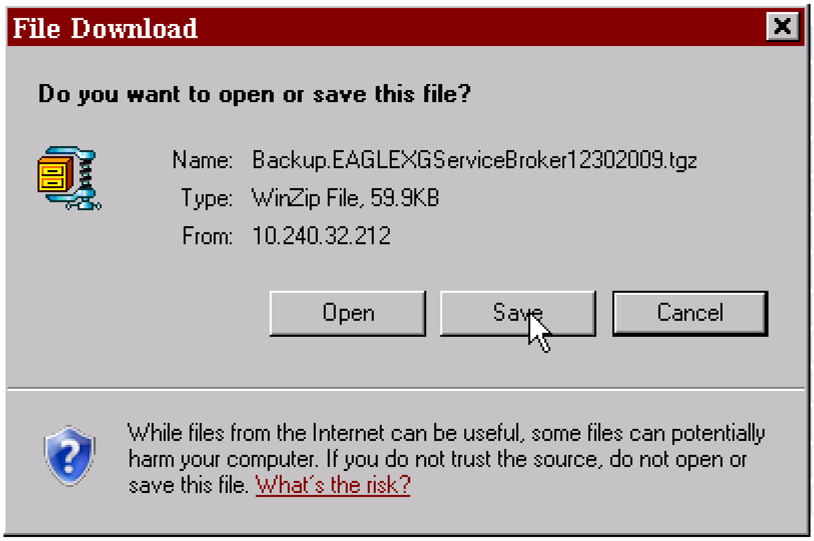
1. **Click on the file link as shown and click the Download button**



Displaying Entries 1-12 of 12 | First | Prev | Next | Last |

Action	Filename	Size	TimeStamp	Action
Delete	872-1734-02-2.0.0_20.30.0-i386.iso	479.4 MB	2009-Dec-18 11:22:03 UTC	Delete
Delete	872-1734-02-2.0.0_20.31.0-i386.iso	480.1 MB	2009-Dec-24 05:42:14 UTC	Delete
Delete	AppNet.xml	4.2 KB	2009-Dec-03 14:53:05 UTC	Delete
Delete	Backup.EAGLEXGServiceBroker12302009.tgz	60 KB	2009-Dec-30 21:18:46 UTC	Delete
Delete	Events_20091208_115716.csv	1.1 MB	2009-Dec-08 11:57:17 UTC	Delete
Delete	Events_20091221_133401.csv	4.2 MB	2009-Dec-21 13:34:03 UTC	Delete
Delete	Events_20091228_152105.csv	5 MB	2009-Dec-28 15:21:08 UTC	Delete
Delete	TKLCConfigData.sh	1.4 KB	2009-Dec-03 15:25:58 UTC	Delete
Delete	Upgrade.Backup.TekSCIM-2.0.0_20.30.0.20091218_071704	369.3 KB	2009-Dec-18 12:17:04 UTC	Delete
Delete	Upgrade.Backup.TekSCIM-2.0.0_20.31.0.20091224_013917	407 KB	2009-Dec-24 06:39:18 UTC	Delete
Delete	ugwrap.log	2.6 KB	2009-Dec-24 06:47:36 UTC	Delete
Delete	upgrade.log	78.3 KB	2009-Dec-24 06:47:36 UTC	Delete

2. **File download dialog box will be displayed as shown, click on the save button and save it to local machine:**



Do you want to open or save this file?

Name: Backup.EAGLEXGServiceBroker12302009.tgz
Type: WinZip File, 59.9KB
From: 10.240.32.212

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

5.6	**Upload the image to secure location for future disaster recovery of entire system.**	Transfer the backed up image file from the previous step to a secure location where the Server Backup files are fetched in case of system disaster recovery.
6.6	**Database Backup Complete**	Database backup of the Eagle XG DSR 3.0 / 4.x 2-tier complete.

Appendix B.

Recovering/Replacing a Failed 3rd party components (Switches, OAs)

Procedure 4: Recovering a failed Aggregation PM&C Server

STEP #	The intent of this procedure is to recover a failed PM&C Server Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	
1.		Refer to [6] *PM&C 3.0 Disaster Recover* on instructions how to recover a PM&C Server. Once the pmac server is recovered, Execute in [5], procedure 4, steps 1 and 2.

Procedure 5: Recovering a failed Aggregation Switch (Cisco 4948E / 4948E-F)

STEP #	The intent of this procedure is to recover a failed Aggregation (4948E / 4948E-F) Switch. Prerequisites for this procedure are: • A copy of the networking xml configuration files • A copy of HP Misc Firmware DVD or ISO Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	

1.		Refer to [4], procedure "**Replace a failed 4948/4948E/4948E-F switch (c-Class system) (netConfig)**", to replace a failed Aggregation switch. You will need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files, which can be found on the PM&C server, under
		`/usr/TKLC/smac/etc/4948E_L3_template_configure.xml`
		`/usr/TKLC/smac/etc/switch1A_4948E_cClass_template_init.xml`
		`/usr/TKLC/smac/etc/switch1BA_4948E_cClass_template_init.xml`

Procedure 6: Recovering a failed Enclosure Switch (Cisco 3020)

S T E P #	The intent of this procedure is to recover a failed Enclosure (3020) Switch. Prerequisites for this procedure are: • A copy of the networking xml configuration files • A copy of HP Misc Firmware DVD or ISO Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	

1.		Refer to [4], procedure "**Reconfigure a failed 3020 switch(netConfig)**", to replace a failed Enclosure switch. You will need a copy of the original networking xml files, which can be found on the PM&C server, under
		`/usr/TKLC/smac/etc/3020_template_configure.xml`
		`/usr/TKLC/smac/etc/3020_template_init.xml`

Procedure 7: Recovering a failed Enclosure Switch (HP 6120XG)

S T E P #	The intent of this procedure is to recover a failed Enclosure (6120XG) Switch. Prerequisites for this procedure are: • A copy of the networking xml configuration files A copy of HP Misc Firmware DVD or ISO Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	

1.		Refer to [4], procedure "**Reconfigure a failed HP 6120XG switch (netConfig)**", to replace a failed Enclosure switch. You will need a copy of the original networking xml files, which can be found on the PM&C server, under
		`/usr/TKLC/smac/etc/6120XG_template_configure.xml`
		`/usr/TKLC/smac/etc/6120XG_template_init.xml`

Procedure 8: Recovering a failed Enclosure OA

S T E P #	The intent of this procedure is to recover a failed Enclosure Onboard Administrator Switch. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.

1.		Refer to [4], procedure "**Replacing Onboard Administrator in a system with redundant OA"** to replace a failed Enclosure OA.

Appendix C. Workarounds for Issues/PR not fixed in this release

Issue	Associated PR	Workaround

Inetmerge alarm after force restore	222826	Get the clusterID of the NO using the following command: # **top.myrole** *myNodeId=**A3603**.215* *myMasterCapable=true* ... Then update the clusterId field in RecognizedAuthority table to have the same clusterid: # **ivi RecognizedAuthority**
Incorrect NodeID		
Inetrep alarm after performing disaster recovery	222827	Restart the Inetrep service on all affected servers using the following commands: # **pm.set off inetrep** # **pm.set on inetrep**
Inetsync alarms after performing disaster recovery	222828	Restart the Inetsync service on all affected servers using the following commands: # **pm.set off inetsync** # **pm.set on inetsync**
Active NO /etc/hosts file does not contain server aliases after force restore done	222829	Update the /etc/hosts file with the missing entries (or copy it from another server (e.g. SO) if it is complete on that server)
Active NO cannot communicate with other Servers		

Appendix D. Contacting Tekelec

Disaster recovery activity may require real-time assessment by Tekelec Engineering in order to determine the best course of action. Customers are instructed to contact the Tekelec Customer Care Center (CCC) for assistance if an enclosure FRU is requested. The CCC may be reached using the following contact information:

Tekelec Customer Care Center

US: 1-888-367-8552