Oracle® Communications Diameter Signaling Router

DSR 4.X/5.X 3-tier Disaster Recovery Guide

Release 5.1

909-2246-001

December 2013

ORACLE®

Oracle Communications Diameter Signaling Router 3-tier Disaster Recovery Procedure, Release 5.1

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

FAX: 919-460-2126

TABLE OF CONTENTS

List of Figures

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 4.x/5.x (3-tier deployments). This includes recovery of partial or a complete loss of one or more DSR 4.x/5.x servers. The audience for this document includes GPS groups such as 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 4.x/5.x. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note that components dependent 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. ([10] for SDS and [19] chapter 6 for DIH)

Note that this document only covers the disaster recovery scenarios of 3-tier deployments. For 2-tier deployments, refer to [12] for the proper disaster recovery procedures.

1.2 References

[1] *HP Solutions Firmware Upgrade Pack*, 795-0000-2xx, v2.2.x (latest recommended, 2.2.4 minimum)

[2] *Diameter Signaling Router 4.x/5.x Networking Interconnect Technical References*, TR007133/4/5/6/7/8/9

[3] *TPD Initial Product Manufacture*, 909-2130-001

[4] *Platform 6.x Configuration Procedure Reference*, 909-2249-001

[5] *DSR 4.x HP C-class Installation*, 909-2228-001

[6] *DSR 5.x Base Hardware and Software Installation*, 909-2282-001

[7] *DSR 5.x Software Configuration*, 909-2278-001

[8] *PM&C 5.x Disaster Recover*, 909-2210-001

[9] *Appworks Database Backup and Restore*, UG005196

[10] *SDS 3.x Disaster Recovery Guide*, TR007061

[11] *XIH 5.0 Installation and Upgrade Procedure*, 909-2265-001

[12] *DSR 3.0/4.x/5.x 2-tier Disaster Recovery*, 909-2225-001

[13] *Policy DRA Activation*, WI006835

[14] *CPA Activation Feature Work Instruction*, WI006780, latest version, Fisher

[15] *IPFE Installation and Configuration*, WI006837, latest version, Mahoney

[16] *DSR Meta Administration Feature Activation*, WI006761, latest version, Fisher

[17] *DSR FABR Feature Activation*, WI006771, latest version, Karmarkar

[18] *DSR RBAR Feature Activation*, WI006763, latest version, Fisher

[19] *DIH 5.0 Disaster Recovery Procedure*, 909-2266-001, latest version, Tekelec 2013

[20] *IPFE 3.0 Feature Activation and Configuration*, WI006931, latest version, Mahoney

1.3 Software Release Numbering

This procedure applies to all EAGLE XG DSR 4.x/5.x releases.

1.4 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

1.5 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 4.x/5.x disaster recovery procedure falls into four basic categories. It is primarily dependent on the state of the Network OAM&P servers and System OAM servers:

- Recovery of the entire network from a total outage
  - Both NO servers failed
  - All SO servers failed
- Recovery of one or more servers with at least one Network OAM&P server intact
  - 1 or both NO servers intact
  - 1 or more SO or MP servers failed
- Recovery of the Network OAM&P pair with one or more System OAM servers intact
  - Both NO servers failed
  - 1 or more SO servers intact
- Recovery of one or more servers with at least one Network OAM&P and one Site OAM server intact
  - 1 or both NO servers intact
  - 1 or more SO servers intact
  - 1 SO or 1 or more MP servers failed

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

For DIH recovery, refer to [19].

2.1 Complete Server Outage (All servers)

This is the worst case scenario where all the servers in the network have suffered complete software and/or hardware failure. The servers are recovered using base recovery of hardware and software and then restoring database backups to the active NO and SO servers. 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 files are 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 one NO Server Intact and both SOs failed

This case assumes that one or both Network OAM&P servers intact. All servers have failed and are recovered using base recovery of hardware and software. Database is restored on the SO and replication will recover the database of the remaining servers.

2.3 Partial Server Outage with both NO Servers failed and one SO server Intact

If both Network OAM&P servers have suffered complete software and/or hardware failure but at least one System OAM server is available, recovery is aided by extracting replicated data from the SO server. The extracted data is restored to the rebuilt Network OAM&P server(s). NOTE: some data on the Network OAM&P servers is not replicated to System OAM server (and cannot be restored automatically) and therefore must be reentered manually. This is described later in this document.

2.4 Partial Server Outage with one NO and one SO Server Intact

The simplest case of disaster recovery is with one or both Network and Site OAM&P servers intact. All servers are recovered using base recovery of hardware and software. Database replication from the active NO and SO servers will recover the database to all servers. (Note: this includes failures of any disaster recovery Network NOAM&P 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 (909-2246-001) and hardcopies of all documents in the reference list: [1] through [7].
2. Hardcopy of all site surveys performed at the initial installation and network configuration of this customer's site.. 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 4.x/5.x backup files: electronic backup file (preferred) or hardcopy of all DSR 4.x configuration and provisioning data. Check [9] 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 (64 bits).
6. Platform Management & Configuration (PM&C) CD-ROM.
7. EAGLE XG DSR 4.x/5.x CD-ROM (or ISO image file on USB Flash) of the target release.
8. TVOE Platform Media (64 bits)
9. The xml configuration files used to configure the switches, available on the PM&C Server.
10. The network element XML file used for the blades initial configuration.
11. The HP firmware upgrade Kit
12. NetBackup Files if they exist. This may require the assistance of the customer's NetBackup administrator.

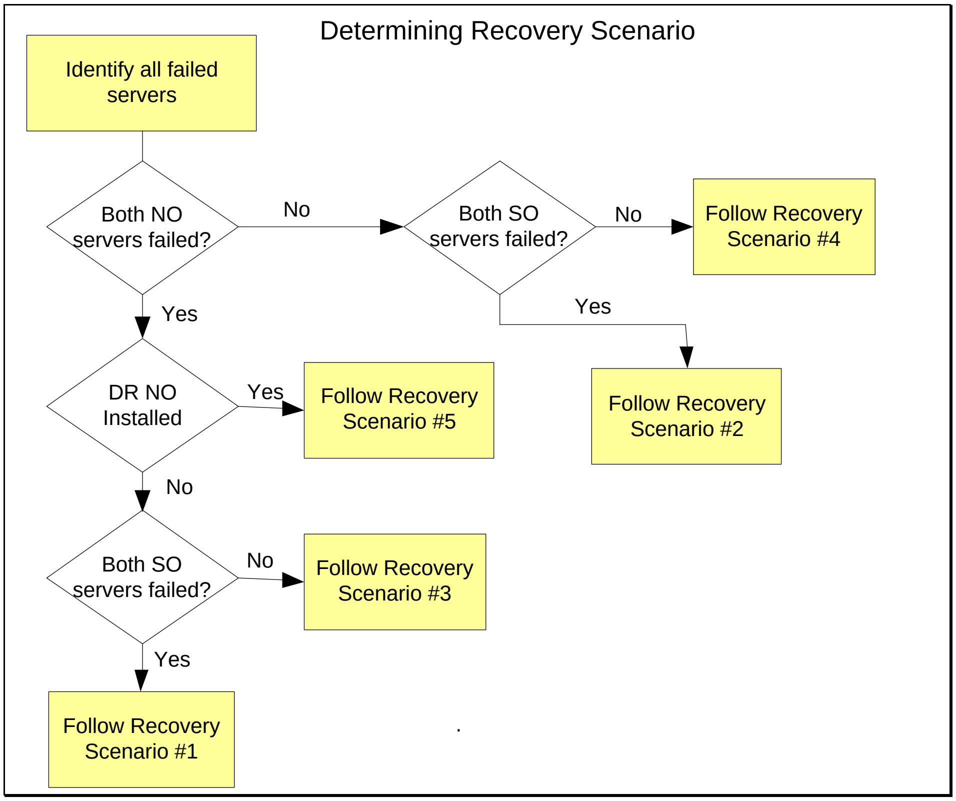
For all Disaster Recovery scenarios, we assume that the NO Database backup and the SO Database backup were performed around the same time, and that no synchronization issues exist among them.

3.2 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 Figure 1 and Table 2).
5. Execute appropriate recovery procedures (listed in Table 2).

Figure 1: Determining Recovery Scenario


Determining Recovery Scenario
Identify all failed servers
Both NO servers failed?
No
Both SO servers failed?
No
Follow Recovery Scenario #4
Yes
Yes
DR NO Installed
Yes
Follow Recovery Scenario #5
Follow Recovery Scenario #2
No
Both SO servers failed?
No
Follow Recovery Scenario #3
Yes
Follow Recovery Scenario #1

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. • All SO servers failed. • MP servers may or may not be failed.	Execute Section 5.1.1, Procedure 1.
2	• At least 1 NO server is intact and available. • All SO servers failed. • MP servers may or may not be failed.	Execute Section 5.1.2, Procedure 2.
3	• Both NO servers failed. • At least 1 SO server is intact and available. • MP servers may or may not be failed.	Execute Section 5.1.3, Procedure 3.
4	• At least 1 NO server is intact and available. • At least 1 SO server is intact and available. • 1 or more MP servers have failed.	Execute Section 5.1.4, Procedure 4.
5	• Both NO servers failed. • DR NO is Available • SO servers may or may not be failed. • MP servers may or may not be failed.	Execute Section 5.1.4, Procedure 5.

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 bv Tekelec.
2. Base Hardware Replacement must be controlled by engineer familiar with DSR 4.x Application.

5.1 Recovering and Restoring System Configuration

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

5.1.1 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] for DSR 4.x or reference [6] for DSR 5.x).
    - Recover the Virtual Machines hosting the NOs and SOs. (by executing procedures from reference [5] for DSR 4.x or reference [6] for DSR 5.x)
    - Recover the software. (by executing installation procedures, reference [5] for DSR 4.x or reference [6] for DSR 5.x)
- Recover Active NO server by recovering its' NO VM Image.
    - Recover the NO database.
    - Reconfigure the application
- Recover Standby NO server by recovering base hardware and software and/or VM Image.
    - Reconfigure the Application
- Recover all SO and MP servers by recovering base hardware and software.
    - Recover the SO database.
    - Reconfigure the Application
    - Reconfigure the signaling interfaces and routes on the MPs (by executing installation procedures, reference [5] for DSR 4.x or reference [7] for DSR 5.x)
- Restart processes and re-enable provisioning and replication.

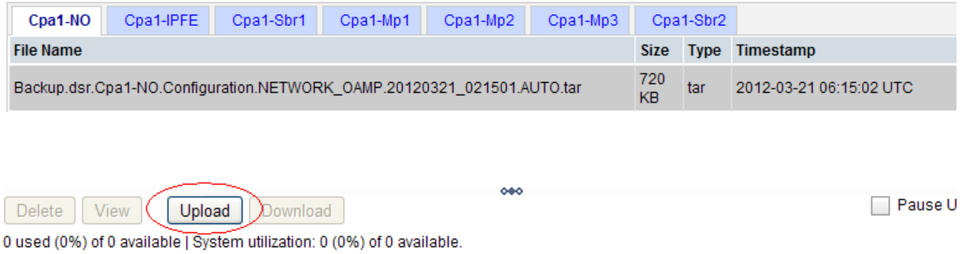
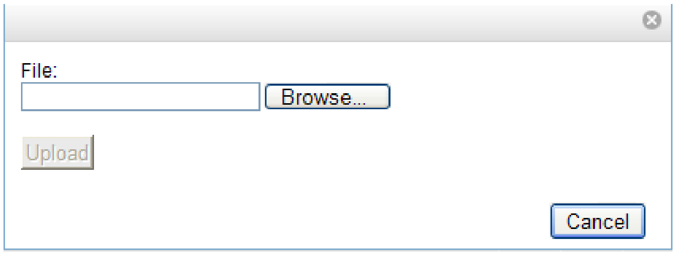
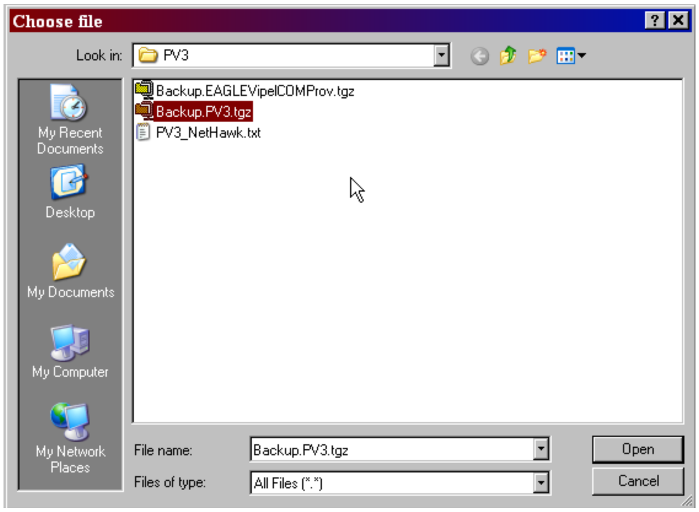
Note that any other applications DR recovery actions (SDS and DIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution (i.e. stale DB on DP servers will not receive updates until SDS-SO servers are recovered

Follow procedure below for detailed steps.

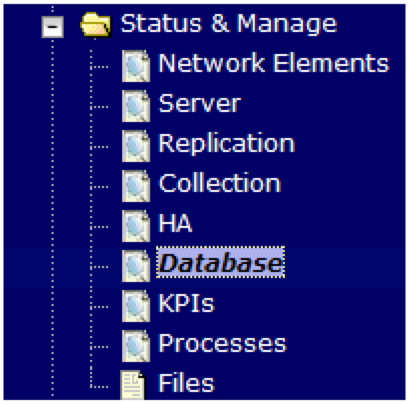
Procedure 1. Recovery Scenario 1

S T E P #	This procedure performs recovery if both NO servers are failed and both SO servers are failed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Note: If any errors are encountered during the execution of this procedure, refer to the list of known issues in Appendix E before contacting Tekelec Customer Support 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 Servers and Blades and install replacements. 3. Configure and verify the BIOS on the Blade. Execute procedure “Confirm/Update Blade Server BIOS Settings” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. 4. Execute Procedure “Configure iLO password for Blades’ Administrator Account” from [5] to setup the root password on the newly installed blade. 5. Load any firmware upgrades using [1]. 6.Execute procedure “Install TVOE on VM Host Server Blades” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. 7.Execute procedure “Configure TVOE on Server Blades” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. 8.Execute procedure “Create NOAMP Guest VMs” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. 9.Execute procedure “Create SOAM Guest VMs” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. 10. IPM all the guests using procedure “IPM Blades and VMs” from [5] for DSR 4.x or reference [7] for DSR 5.x. Instruct any other any other Application’s personnel to start recovery procedures on the Guests hosted by the server (parallel recovery). 11. Install the application on the all the guests using procedure “Install the Application Software on the Blades” from [5] for DSR 4.x or reference [7] for DSR 5.x.. 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 4.x/5.x database backup file. If you are using Netbackup, then co-ordinate with the customer’s Netbackup administrator to retrieve the proper NOAM/SOAM database backup files. 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 4.x/5.x Installation procedures.	Execute the following procedures from the DSR 4.x/5.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. Execute installation procedures for the first NO server. See reference [5] for DSR 4.x or reference [7] for DSR 5.x, Procedure “Configure the First NOAMP Server”, and “Configure the NOAMP Server Group”.
4 □	Login into the NO XMI Address	Log into the first NO GUI.
5	Upload the backed up database file from Remote location into	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 “NO Provisioning and Configuration:” file backed up after initial

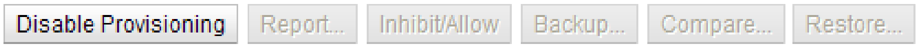
Procedure 1. Recovery Scenario 1

□	File Management Area.	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 Delete View Upload Download □ Pause U 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.  File: Browse... Upload Cancel  Choose file Look in: PV3 Backup.EAGLEVipelCOMProv.tgz Backup.PV3.tgz PV3_NetHawk.txt My Recent Documents Desktop My Documents My Computer My Network Places File name: Backup.PV3.tgz Files of type: All Files (*.*) Open Cancel 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

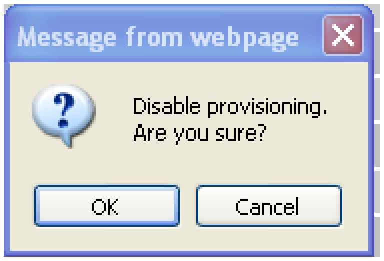
Procedure 1. Recovery Scenario 1



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.

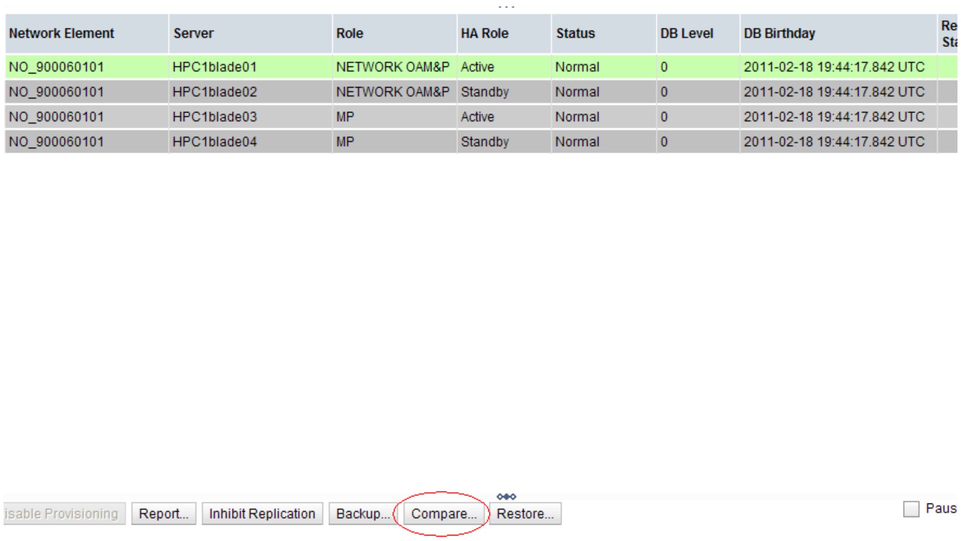


Disable provisioning.
Are you sure?

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

7 □ Verify the Archive Contents and Database Compatibility

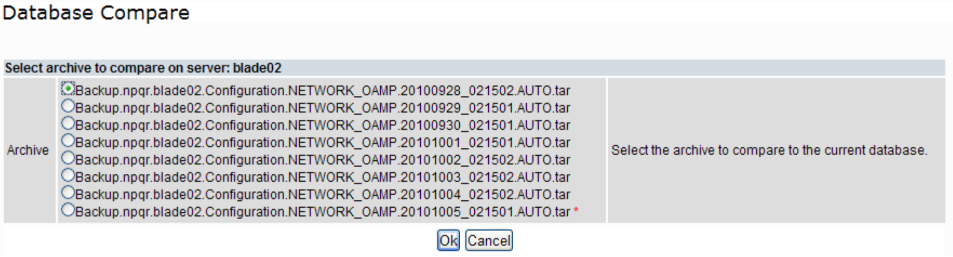
1. Select the Active NO Server and click on the “Compare”:



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.

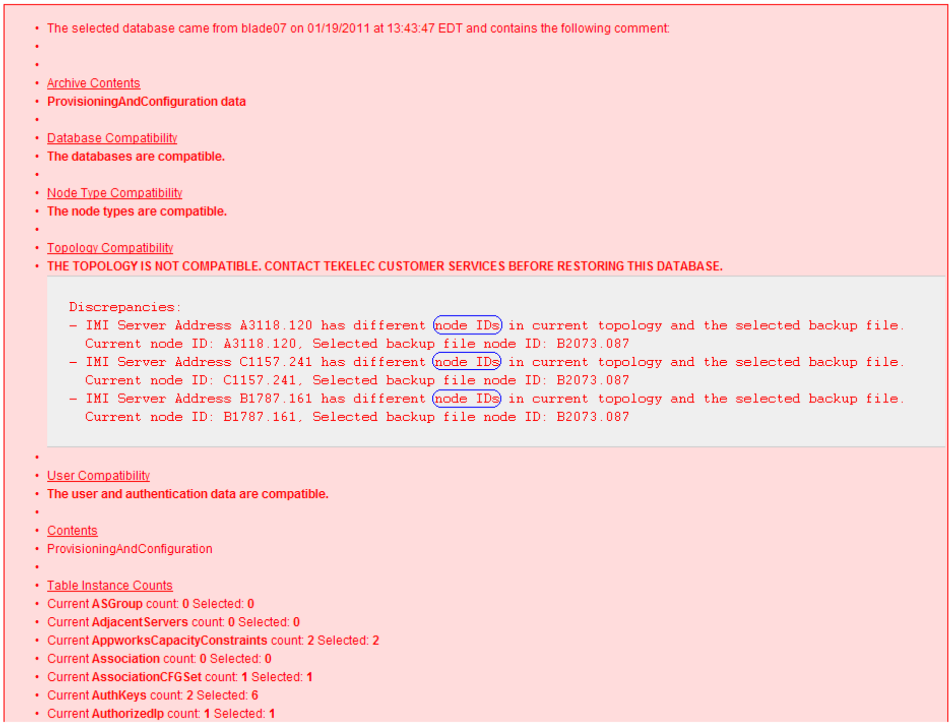


Database Compare

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: Provisioning and 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.

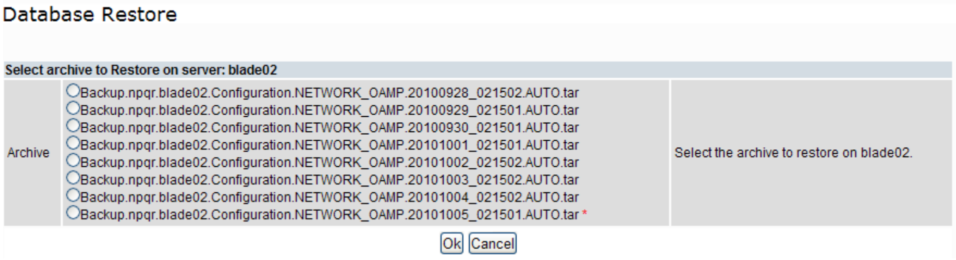
4. If the verification is successful, Click BACK button and continue to next step in this

Procedure 1. Recovery Scenario 1

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

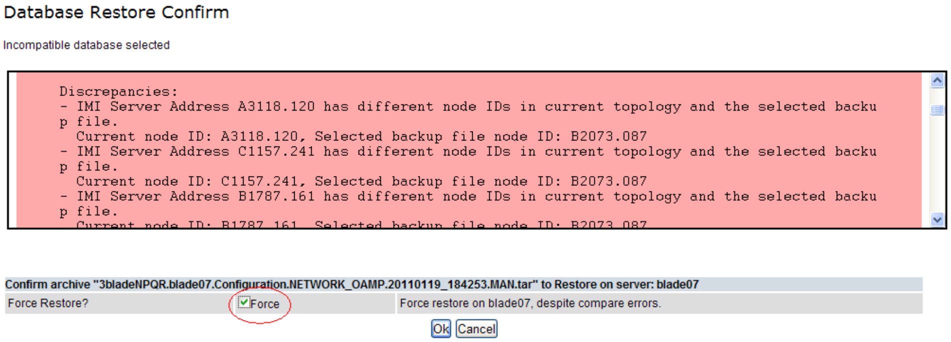


Database Restore

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

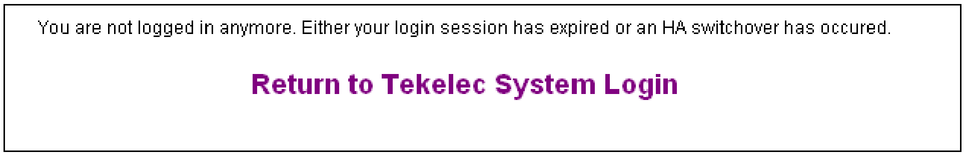
Incompatible database selected

```
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.

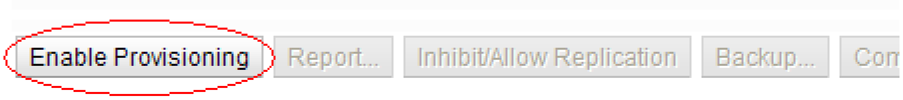
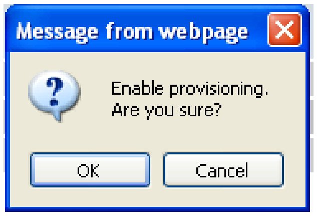
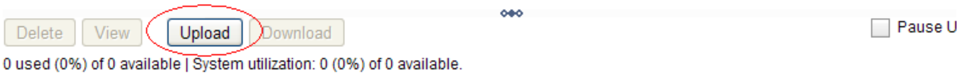
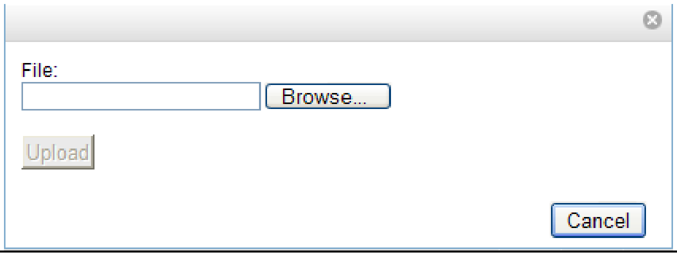
7. Log in Back into GUI using VIP address by clicking “Continue to this Website”
8. Login using the guiadmin login and password into the GUI
9. Wait for 5-10 minutes for the System to stabilize with the new topology: Monitor the Info tab for “Success”. This will indicate that the backup is complete and the system is stabilized.
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)

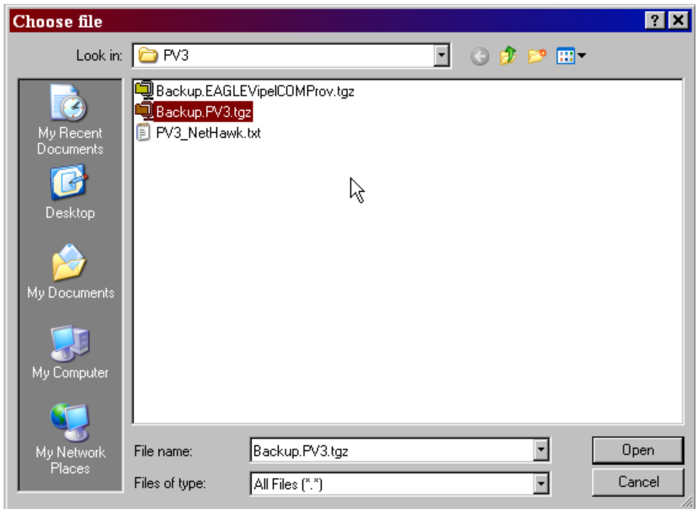
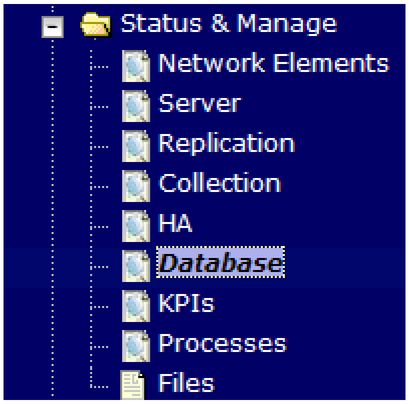
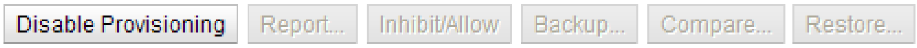
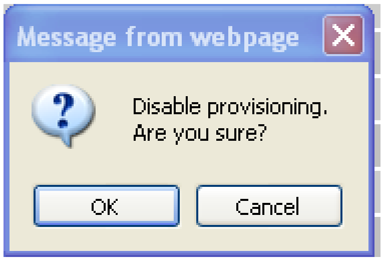
Do not pay attention to alarms until all the servers in the system are completely restored.

NOTE: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.

Procedure 1. Recovery Scenario 1

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.  Enable provisioning. Are you sure?
10 □	Recover standby NO server.	Recover the standby NO server: 1. Install the second NO server by executing Reference [5] for DSR 4.x or reference [7] for DSR 5.x, Procedure “Configure the Second NOAMP Server, steps 1, 4, 5 and 6”. If Netbackup is used, execute Procedure 35 from [5] or Procedure 13 from [7].
11 □	Recover active SO server.	Recover the active SO server: 1. Install the SO servers by executing Reference [5] for DSR 4.x or reference [7] for DSR 5.x, Procedure “Configure the SOAM Servers”, steps 1, 4, 5, 6.,7. If you are using Netbackup, also execute step 10.
12 □	Upload the backed up SO database file from Remote location into File Management Area.	1. Browse to Main Menu->Status & Manage->Files 2. Select the Active SO Server. The following screen will appear. Click on “Upload” as shown below and select the file “SO Provisioning and Configuration:” file backed up after initial installation and provisioning.  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. 

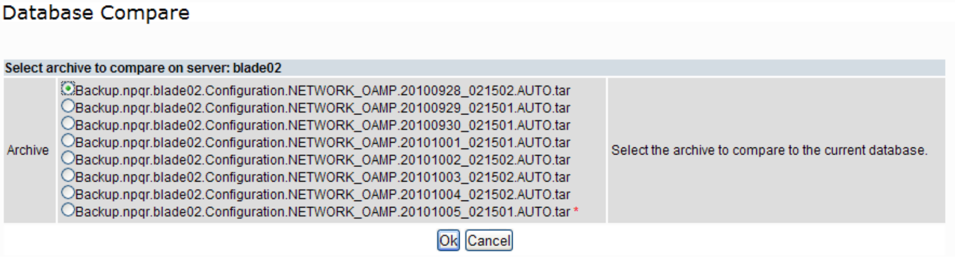
Procedure 1. Recovery Scenario 1

		 Choose file My Recent Documents Desktop My Documents My Computer My Network Places Open Cancel Look in: PV3 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.
13 □	Disable Provisioning	1. Click on Main Menu->Status & Manage->Database  Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files 2. Disable Provisioning by clicking on “Disable Provisioning” button at the bottom of the screen as shown below.  Disable Provisioning Report... Inhibit/Allow Backup... Compare... Restore... 3. A confirmation window will appear, press “OK” to disable Provisioning.  Message from webpage Disable provisioning. Are you sure? 4. The message “Warning Code 002” will appear.

Procedure 1. Recovery Scenario 1

14 □ Verify the Archive Contents and Database Compatibility

1. Login onto the recently recovered Active SO GUI
2. Click on Main Menu->Status & Manage->Database
3. Select the Active SO Server and click on the “Compare”:
4. 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

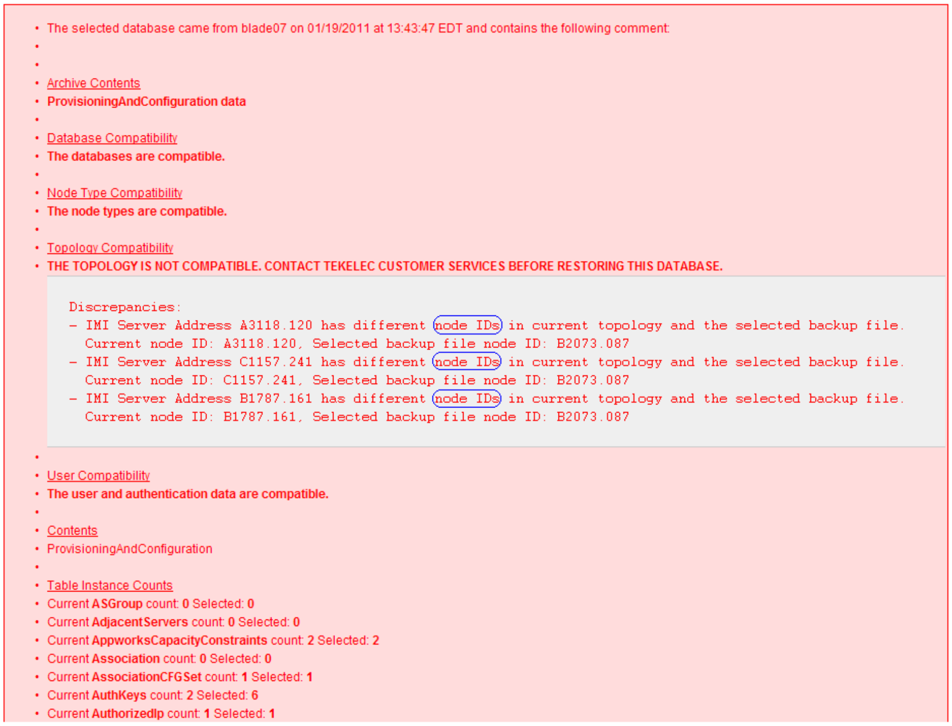
Select archive to compare on server: blade02

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.

5. 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**

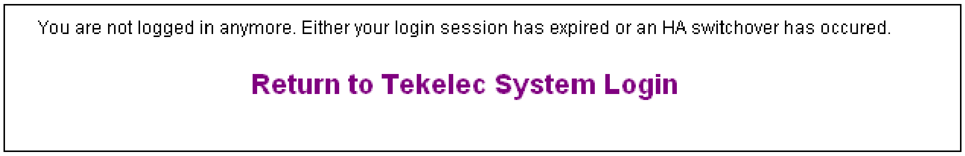
NOTE: Archive Contents and Database Compatibilities must be the following:

Archive Contents: Provisioning and Configuration data

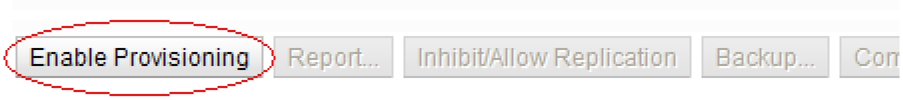
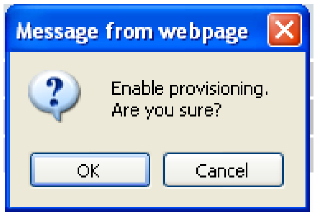
Database Compatibility: The databases are compatible.

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

Topology Compatibility

		THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **NOTE:** We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility. 6. If the verification is successful, Click BACK button and continue to next step in this procedure. NOTE: Please refer to the workarounds in Appendix E if any problems are encountered in this step.
15 □	Restore the Database	1. SSH to the SO terminal as **root** 2. Verify that the SO database backup file that was uploaded in step 12 is located under **/var/TKLC/db/filemgmt** by running the following command: # **ls /var/TKLC/db/filemgmt/<filename>** 3. Depending on the type of the backup file, restore it using one of the following commands: If the file is a bzip2 compressed tar file (extension is .tar.bz2): # **idb.restore -f –j <filename>** If the file is a gzip compressed tar file (extension is .tar.gz): # **idb.restore -f –z <filename>** If the file an uncompressed tar file (extension is .tar): # **idb.restore –f –n <filename>** 4. Wait for the restore to finish, it should take a few minutes, and check the output for errors. If errors were present, contact Tekelec customer support. The following truncated output is expected: … *- Reinitialize MySQL* *- Unlocking idbsvc for each part* *- Sync Parts to disk* 5. **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** 6. Log in Back into GUI VIP by clicking "Continue to this Website" 7. Login using the guiadmin login and password into the GUI 8. Wait for 5-10 minutes for the System to stabilize with the new topology. 9. 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 SOAM), "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.***

Procedure 1. Recovery Scenario 1

16 □	Re-enable Provisioning	1. Log into the Active NO GUI 2. Click on Main Menu->Status & Manage->Database menu item.  Enable Provisioning Report... Inhibit/Allow Replication Backup... Con 3. 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?
17 □	Restore /etc/hosts file of active NO	**Release 5.X:** From the recovered NO server command line, execute: `# AppWorks AppWorks_AppWorks updateServerAliases <NO Host Name>` **Release 4.X:** 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)
18 □	Recover remaining SO servers.	Recover the remaining SO servers (standby, spare) by repeating the following step for each SO Server: 1. Install the second SO server by executing Reference [5] for DSR 4.x or reference [7] for DSR 5.x, Procedure “Configure the SOAM Servers”, steps 1, 4, 5, and 6”. Execute step 10 as well if Netbackup is used.
19 □	Recover the MP Servers (Also applies to IPFE)	Execute the following procedures from [5] for DSR 4.x or reference [7] for DSR 5.x FOR **EACH** MP that has been recovered: 1.”Configure MP Blades Servers”, Steps 1, 5,6,7,8,9. 2. **FOR DSR 4.X *ONLY* :** 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>** 3 If IPFE servers are being recovered, execute Procedure 5 of [20] for any applicable IPFE servers.
20 □	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.
21 □	**DSR 5.X Recovery Only:** Re-Sync NTP if Necessary (Optional)	Navigate to **Status & Manage** -> **Server,** then select each server that has been recovered and click **NTP Sync**.

Procedure 1. Recovery Scenario 1

22 □ 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 SOAM Server

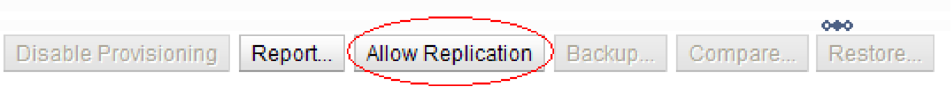
   d. Standby SOAM Server

   e. Spare SOAM Server (if applicable)

   f. Active DR NOAM Server

   g. MP/IPFE Servers (if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter)

   h. 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”.

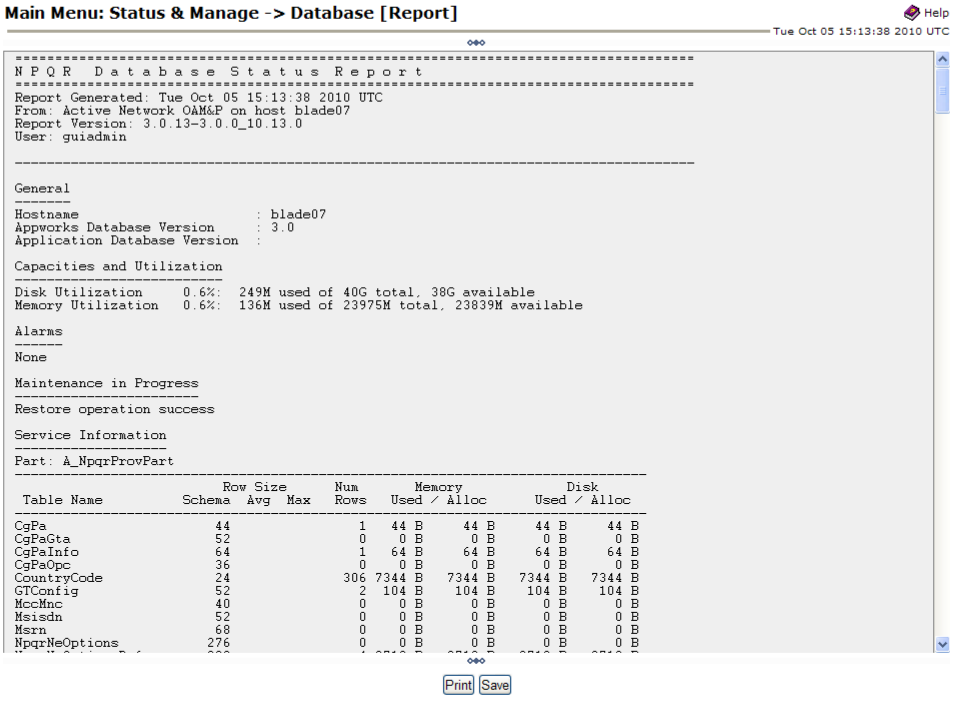


23 □ Remove Forced Standby

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**

24 □ 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.

Procedure 1. Recovery Scenario 1

25 □ **DSR 4.X Recovery ONLY:** Optimize Comcol memory usage on NO and SO

If recovering a DSR 4.x system, execute this step, otherwise skip to step 25.

Obtain a terminal window connection to the (NO/SO) server console via SSH or iLO. **If using SSH, use the actual IP of the server, not the VIP address.**

Execute the following on the command line. Wait until the script completes and you are returned to the command line:

```
# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage
# sleep 20
# prod.start
# pm.sanity
Sanity check OK: 01/23/13 11:42:20 within 15 secs
```

Verify that the script finished successfully by checking the exit status:

```
# echo $?
```

If anything other than “0” is printed out,. halt this procedure and contact Tekelec Support..

Repeat this step for the **standby NO, D.R. NO (if applicable) servers, and every SO server at every site.**

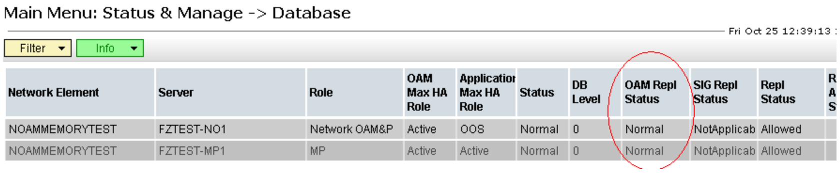
26 □ **DSR 4.X Recovery ONLY:** Optimize Comcol memory usage on DA-MP

SSH to each DA-MP and execute the following command. Note that this command **SHOULD NOT** be executed on SBR blades.

```
# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force
```

27 □ Verify Replication between servers.

1. Click on Main Menu->Status and Manager->Replication
2. Verify that replication is occurring between servers Server.



Main Menu: Status & Manage -> Database

Fri Oct 25 12:39:13 :

Network Element	Server	Role	OAM Max HA Role	Applicatior Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	R A S
NOAMMEMORYTEST	FZTEST-NO1	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicab	Allowed	
NOAMMEMORYTEST	FZTEST-MP1	MP	Active	Active	Normal	0	Normal	NotApplicab	Allowed	

28 □ Verify the Database states

1. Click on Main Menu->Status and Manager->Database
2. Verify that the HA Role is either “Active” or “Standby”, and that the status is “Normal”.

29 □ Verify the HA Status

1. Click on Main Menu->Status and Manager->HA
2. Check the row for all the MP Server
3. Verify that the HA Role is either Active or Standby.

30 □ Verify the local node info

1. Click on Main Menu->Diameter->Configuration->Local Node
2. Verify that all the local nodes are shown.

31 □ Verify the peer node info

1. Click on Main Menu->Diameter->Configuration->Peer Node
2. Verify that all the peer nodes are shown.

Procedure 1. Recovery Scenario 1

32 □	Verify the Connections info	1. Click on Main Menu->Diameter->Configuration->Connections 2. Verify that all the peer nodes are shown.
33 □	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.
34 □	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.
35 □	Restore GUI Username s and passwords	If applicable, Execute steps in Section 6 to recover the user and group information restored.
36 □	Re-activate Optional Features	If optional features (CPA, PDRA, SBR) were activated, they will need to be de-activated and then re-activated. Refer to the [13], [14], [15], [16], [17] or [18] for the appropriate documentation.
37 □	Clear Browser Cache	If the system was restored with DSR 3.0 after running 4.X/5.X, the browser cache needs to be cleared. To do so in IE, navigate to **Tools** -> **Internet Options** and click on **Delete** under browsing history. (For other browsers, refer to their respective documentation/help on how to do so)
38 □	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

5.1.2 Recovery Scenario 2 (Partial Server Outage with one NO Server intact and both SOs failed)

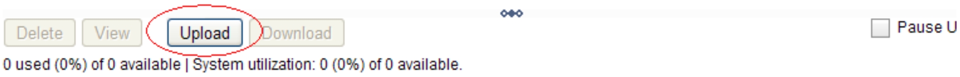
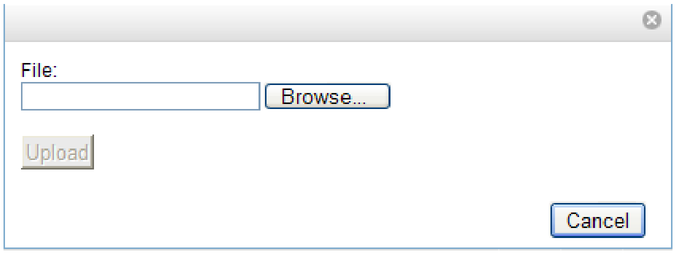
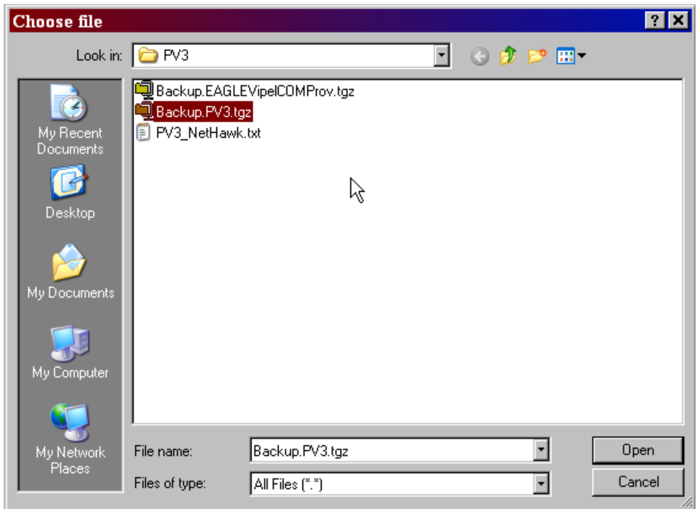
For a partial server outage with an NO server intact and available; SO servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active SO server using a database backup file obtained from the SO servers. All other servers are recovered using recovery procedures of base hardware and software. Database replication from the active NO server will recover the database on these server. 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 needed) by recovering base hardware, software and the database.
  - **Recover** the base **hardware**.
  - **Recover** the **software**.
- Recover Active SO server by recovering base hardware and software.
  - **Recover** the base **hardware**.
  - **Recover** the **software**.
  - **Recover** the **Database**.
- Recover any failed SO and MP/IPFE servers by recovering base hardware and software.
  - **Recover** the base **hardware**.
  - **Recover** the **software**.
  - The database has already been restored at the active SO server and does not require restoration at the SO and MP servers.

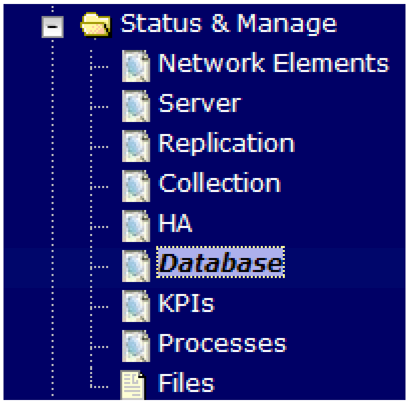
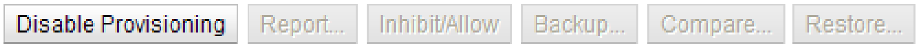
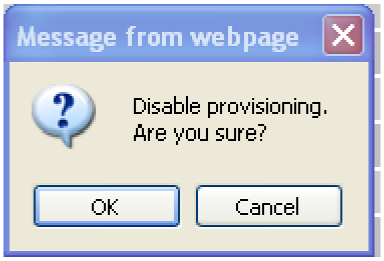
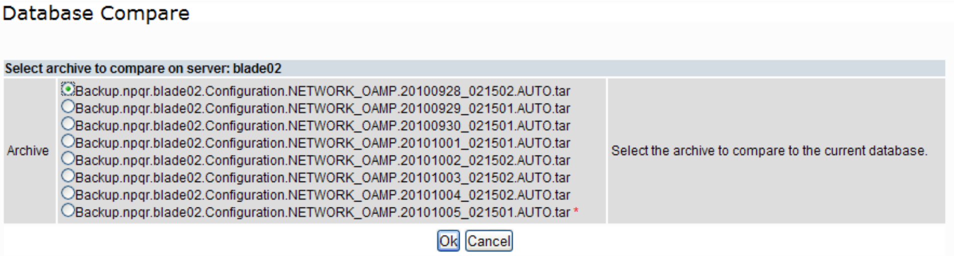
Procedure 2. Recovery Scenario 2

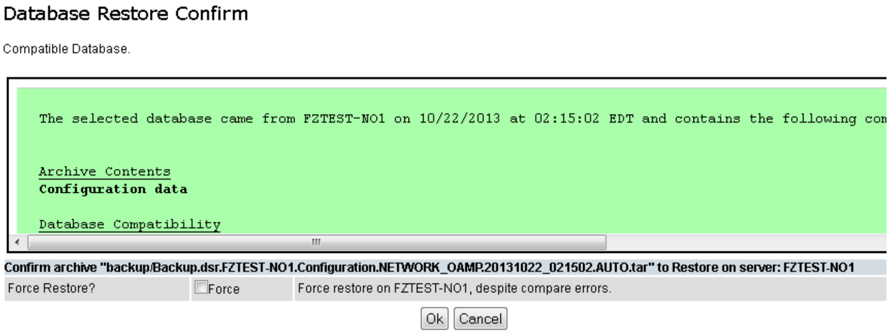
STEP #	This procedure performs recovery if at least 1 NO server is available but both SO servers have failed. This includes any SO server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Note: If any errors are encountered during the execution of this procedure, refer to the list of known issues in Appendix E before contacting Tekelec Customer Support 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, set the server HA state to “Forced Standby” by navigating to Main Menu->HA, then clicking on Edit and setting the “Max Allowed HA Role” to Standby for the NO in question and pressing OK. 3. 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”. 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] for DSR 4.x or reference [6] for DSR 5.x. 6. Execute Procedure “Configure iLO password for Blades’ Administrator Account” from [5] to setup the root password on the newly installed blade. For RMS based servers, execute Appendix I from [3] to configure all iLO settings, including the iLO password. 7. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details. 8. Execute procedure “Install TVOE on Server Blades” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. (Blade-based NOAMPs only) 9. Execute procedure “Configure TVOE on Server Blades” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. (Blade-based NOAMPs only). 10. Execute procedure “Continue TVOE Configuration on First RMS Server” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. (RMS based NOAMPs only) 11. Execute procedure “Configure TOVE on Additional RMS Server(s)” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. (RMS based NOAMPs only) 12. Execute procedure “Create NOAMP Guest VMs” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. 13. 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 . 14. IPM The standby NO using procedure “IPM Blades and VMs” from [5]. or [7] 15. Install the application on the Standby NO using procedure “Install the Application Software on the Blades” from [5] for DSR 4.x or reference [7] for DSR 5.x. 16. Configure the newly installed application by executing procedure “Configure the Second NOAMP Server, from [5] steps 1, 2, 4, 5 and 6. 17. If you are using Netbackup, execute Procedure 35 from [5] or Procedure 13 from [7], “Install Netbackup Client” 18. 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”. 19. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered server and Clicking on “Restart”.

Procedure 2. Recovery Scenario 2

2 □	Recover Active SO servers.	Recover the SO servers: 1. Remove the failed HP c-Class Blade and install the replacement into the enclosure. 2. Configure and verify the BIOS on the Blade. Execute procedure "Confirm/Update Blade Server BIOS Settings" from reference [5] for DSR 4.x or reference [6] for DSR 5.x. 3. Execute Procedure "Configure iLO password for Blades' Administrator Account" from [5] to setup the root password on the newly installed blade. 4. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details. 5. Execute procedure "Install TVOE on Server Blades" from reference [5] for DSR 4.x or reference [7] for DSR 5.x. 6. Execute procedure "Configure TVOE on Server Blades" from reference [5] for DSR 4.x or reference [7] for DSR 5.x. 7. IPM the SO servers using the procedure "IPM Blades and VMs" from [5]. or [7]. 8. Install the SO servers by executing Reference [5] for DSR 4.x or reference [7] for DSR 5.x, Procedure "Configure the SOAM Servers", steps 5 - 7". Also execute step #10 if you are using NetBackup on your SOAMs.
3 □	Upload the backed up SO database file from Remote location into File Management Area.	1. From the NO GUI, Browse to Main Menu->Status & Manage->Files 2. Select the Active SO Server. The following screen will appear. Click on "Upload" as shown below and select the file "SO Provisioning and Configuration:" file backed up after initial installation and provisioning.  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.
4	Disable Provisioning	1. From the NO GUI, Click on Main Menu->Status & Manage->Database

Procedure 2. Recovery Scenario 2

□		 Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files 2. Disable Provisioning by clicking on “Disable Provisioning” button at the bottom of the screen as shown below.  Disable Provisioning Report... Inhibit/Allow Backup... Compare... Restore... 3. A confirmation window will appear, press “OK” to disable Provisioning. Message from webpage Disable provisioning. Are you sure? 4. The message “Warning Code 002” will appear.
5 □	Verify the Archive Contents and Database Compatibility	1. Select the Active SO Server and click on the “Compare”: 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.



Database Restore Confirm

Compatible Database.

```
The selected database came from FZTEST-NO1 on 10/22/2013 at 02:15:02 EDT and contains the following com

Archive Contents
Configuration data

Database Compatibility
```

Confirm archive "backup/Backup.dsr.FZTEST-NO1.Configuration.NETWORK_OAMP.20131022_021502.AUTO.tar" to Restore on server: FZTEST-NO1

Force Restore?	□Force	Force restore on FZTEST-NO1, despite compare errors.

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

Archive Contents: Provisioning and 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

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

6 □ Restore the Database

1. SSH to the SO terminal as **root**
2. Verify that the SO database backup file that was uploaded in step 12 is located under **/var/TKLC/db/filemgmt** by running the following command:

   # **ls /var/TKLC/db/filemgmt/<filename>**

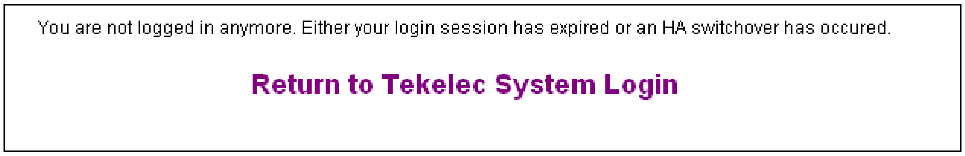
3. Depending on the type of the backup file, restore it using one of the following commands:

   If the file is a bzip2 compressed tar file (extension is .tar.bz2):
   # **idb.restrore -f –j <filename>**

   If the file is a gzip compressed tar file (extension is .tar.gz):
   # **idb.restrore -f –z <filename>**

   If the file an uncompressed tar file (extension is .tar):
   # **idb.restrore -f –n <filename>**

4. Wait for the restore to finish, it should take a few minutes, and check the output for errors. If errors were present, contact Tekelec customer support.
5. **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

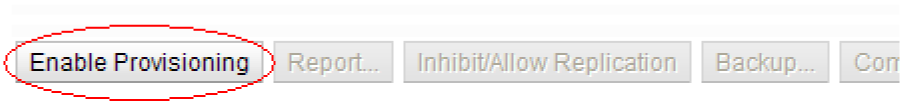
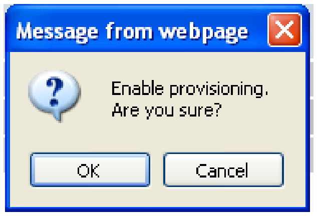


You are not logged in anymore. Either your login session has expired or an HA switchover has occured.

Return to Tekelec System Login

6. Log in Back into GUI VIP by clicking “Continue to this Website”
7. Login using the guiadmin login and password into the GUI
8. Wait for 5-10 minutes for the System to stabilize with the new topology.

Procedure 2. Recovery Scenario 2

		9. 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.***
7 □	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?
8 □	Recover remaining SO servers.	Recover the remaining SO servers (standby, spare) by repeating the following step for each SO Server: 1. Install the second SO server by executing Reference [5] for DSR 4.x or reference [7] for DSR 5.x, Procedure “Configure the SOAM Servers”, steps 1, 4, 5 and 6”.
9 □	Recover the MP Servers (also applies to IPFE servers)	Execute the following procedures from [5] (4.X) or [7] (5.X) FOR **EACH** MP that has been recovered: 1.”Configure MP Blades Servers”, Steps 1, 4, 5, 6 and 7 2. (**DSR 4.X ONLY):** 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>** 3 If IPFE servers are being recovered, execute Procedure 5 of [20] for any applicable IPFE servers.
10 □	**DSR 5.X Recovery Only:** Re-Sync NTP if Necessary (Optional)	Navigate to **Status & Manage** -> **Server,** then select each server that has been recovered and click **NTP Sync**..
11 □	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.

Procedure 2. Recovery Scenario 2

12 □ 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.:

   i. Active NOAMP Server

   j. Standby NOAMP Server

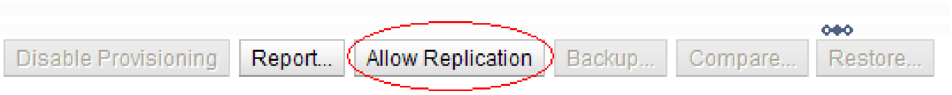
   k. Active SOAM Server

   l. Standby SOAM Server

   m. Spare SOAM Server (if applicable)

   n. Active DR NOAM Server

   o. MP/IPFE Servers (if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter)



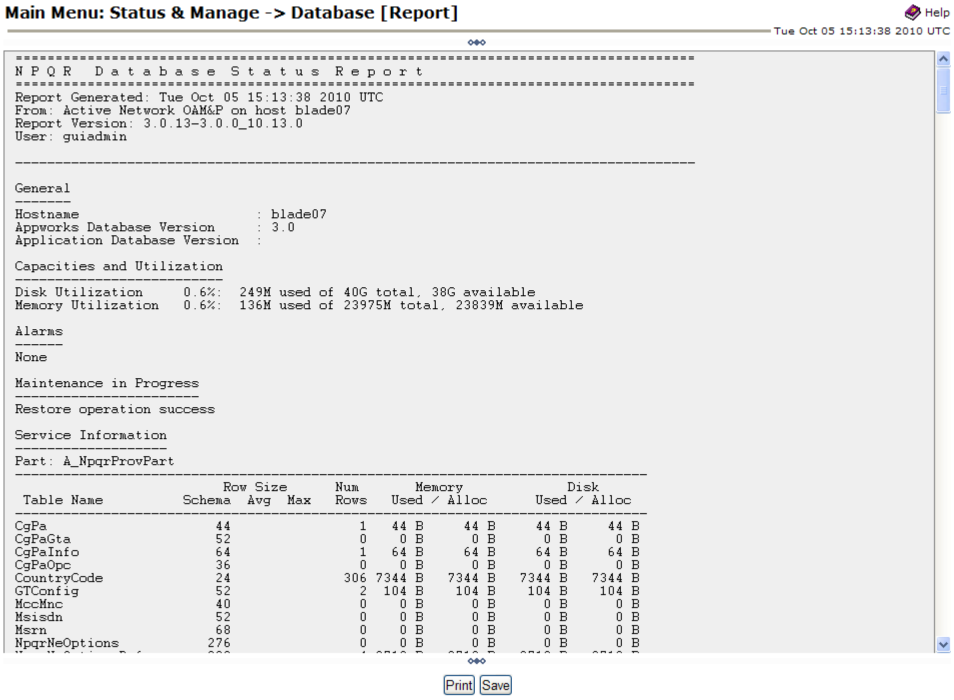
Verify that the replication on all servers is allowed. This can be done by clicking on each server and checking that the button below shows “Inhibit” Replication” instead of “Allow Replication”.

13 □ Remove Forced Standby

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**

14 □ 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:

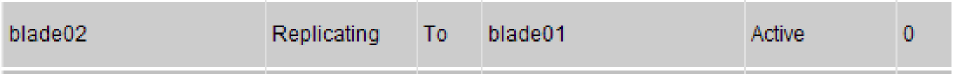

Main Menu: Status & Manage -> Database [Report]
Help
Tue Oct 05 15:13:38 2010 UTC
Print
Save

```
=====================================================================================
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.

Procedure 2. Recovery Scenario 2

15
□
	Optimize Comcol memory usage on recovered NO and SO	If recovering a DSR 4.x system, execute this step, otherwise skip to step 16.
		For each recovered NO or SO, obtain a terminal window connection to the (NO/SO) server console via SSH or iLO. **If using SSH, use the actual IP of the server, not the VIP address.**
		Execute the following on the command line. Wait until the script completes and you are returned to the command line:
		`# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage`
		`# sleep 20`
		`# prod.start`
		`# pm.sanity`
		`Sanity check OK: 01/23/13 11:42:20 within 15 secs`
		Verify that the script finished successfully by checking the exit status:
		`# echo $?`
		If anything other than “0” is printed out,. halt this procedure and contact Tekelec Support..
		Repeat this step for all recovered **NO and SO servers at every site.**

16 □	Optimize Comcol memory usage on DA-MP	SSH to each recovered DA-MP and execute the following command. Note that this command **SHOULD NOT** be executed on SBR blades. `# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force`
17 □	Verify Replication between servers.	1. Click on Main Menu->Status and Manager->Replication 2. Verify that replication is occurring between servers Server.  blade02 Replicating To blade01 Active 0
18 □	Verify the Database states	1. Click on Main Menu->Status and Manager->Database 2. Verify that the HA Role is either “Active” or “Standby”, and that the status is “Normal”.
19 □	Verify the HA Status	1. Click on Main Menu->Status and Manager->HA 2. Check the row for all the MP Server 3. Verify that the HA Role is either Active or Standby.
20 □	Verify the local node info	1. Click on Main Menu->Diameter->Configuration->Local Node 2. Verify that all the local nodes are listed.
21 □	Verify the peer node info	1. Click on Main Menu->Diameter->Configuration->Peer Node 2. Verify that all the peer nodes are listed.
22 □	Verify the Connections info	1. Click on Main Menu->Diameter->Configuration->Connections 2. Verify that all the peer nodes are listed.

Procedure 2. Recovery Scenario 2

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	If optional features (CPA, PDRA, SBR) were activated, they will need to be de-activated and then re-activated. Refer to the [11], [12], [13], [14], [15] or [16] for the appropriate documentation.
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

5.1.3 Recovery Scenario 3 (Partial Server Outage with both NO Servers failed and one SO Server intact)

For a partial server outage with an SO server intact and available; NO servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active NO server using a NO database backup file obtained from external backup sources such as customer servers or Netbackup.. 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 server. 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 3. The major activities are summarized as follows:

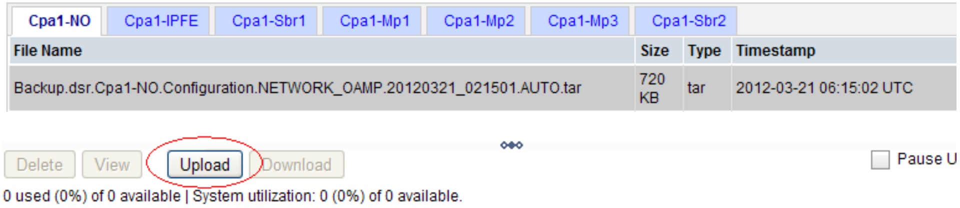
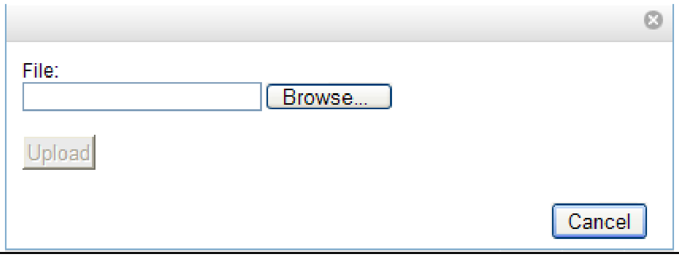
- Recover Active NO server by recovering base hardware, software and the database.
  - **Recover** the base **hardware**.
  - **Recover** the **software**.
  - **Recover** the **database**
- Recover Standby NO server by recovering base hardware and software.
  - **Recover** the base **hardware**.
  - **Recover** the **software**.
  - The database has already been restored at the active NO server and does not require restoration at the standby NO server.
- Recover any failed SO and MP 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 procedure below for detailed steps.

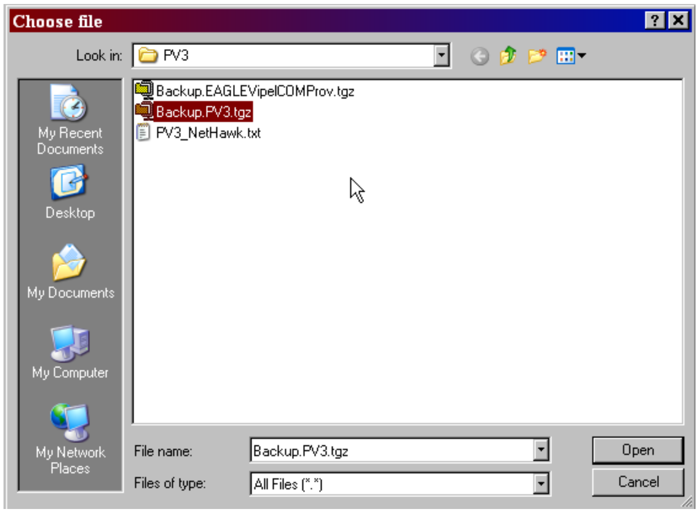
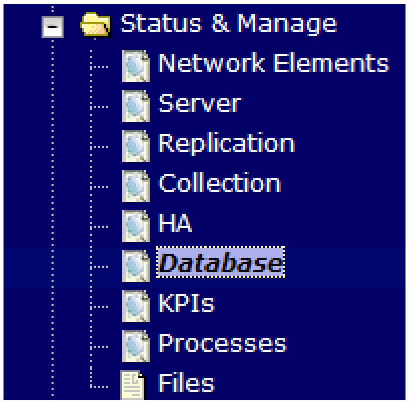
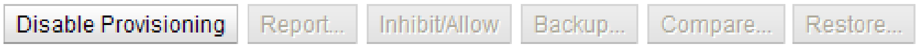
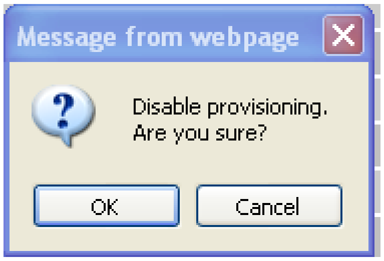
Procedure 3. Recovery Scenario 3

S T E P #	This procedure performs recovery if both NO servers are failed but 1 or more SO servers are intact. This includes any SO server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Note: If any errors are encountered during the execution of this procedure, refer to the list of known issues in Appendix E before contacting Tekelec Customer Support 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: **Note**: If necessary, Refer to [8] *PM&C Disaster Recover* on instructions how to recover a PM&C Server. Gather the documents and required materials listed in Section 3.1. These are the same documents which were required in Step 2. 1. From the NO VIP GUI, set the server HA state to “Forced Standby” by navigating to Main Menu->HA, then clicking on Edit and setting the “Max Allowed HA Role” to Standby for the NO in question and pressing OK. 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. Remove the failed HP c-Class Blade and install the replacement into the enclosure. 4. Configure and verify the BIOS on the Blade. Execute procedure “Confirm/Update Blade Server BIOS Settings” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. 5. Execute Procedure “Configure iLO password for Blades’ Administrator Account” from [5] to setup the root password on the newly installed blade. For RMS based servers, execute Appendix I from [3] to configure all iLO settings, including the iLO password. 6. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details. 7. Execute procedure “Install TVOE on Server Blades” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. (Blade-based NOAMPs only) 8. Execute procedure “Configure TVOE on Server Blades” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. (Blade-based NOAMPs only). 9. Execute procedure “Continue TVOE Configuration on First RMS Server” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. (RMS based NOAMPs only) 10. Execute procedure “Configure TOVE on Additional RMS Server(s)” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. (RMS based NOAMPs only) 11. Execute procedure “Create NOAMP Guest VMs” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. 12. 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 . 13. IPM The standby NO using procedure “IPM Blades and VMs” from [5]. or [7] 14. Install the application on the Standby NO using procedure “Install the Application Software on the Blades” from [5] for DSR 4.x or reference [7] for DSR 5.x. 15. Configure the newly installed application by executing procedure “Configure the Second NOAMP Server, from [5] steps 1, 2, 4, 5 and 6. 16. If you are using Netbackup, execute Procedure 35 from [5] or Procedure 13 from [7], “Install Netbackup Client 17. 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”. 18. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered server and Clicking on “Restart”.

Procedure 3. Recovery Scenario 3

2 ☐	Obtain latest NO database backup and network configuration data.	Obtain the most recent database backup file from external backup sources (ex. file servers, Netbackup) 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 4.x/5.x NO database backup file. If you are using Netbackup, co-ordinate with the customer’s Netbackup administrator to obtain the proper backup files. 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 4.x/5.X Installation procedures.	Execute procedures from EAGLEXG DSR 4.x/5.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. Execute installation procedures for the first NO server. See reference [5] for DSR 4.x or reference [7] for DSR 5.x, Procedure “Configure the First NOAMP Server”, and “Configure the NOAMP Server Group”.
4 ☐	Login into the NO XMI Address	Log into the first NO GUI.
5 ☐	Upload the backed up database file from Remote location into File Management Area.	1. Log into the first NO GUI. 2. Browse to Main Menu->Status & Manage->Files 3. 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 in step 2 above.  Cpa1-NO Cpa1-IPFE Cpa1-Sbr1 Cpa1-Mp1 Cpa1-Mp2 Cpa1-Mp3 Cpa1-Sbr2 Delete View Upload Download Pause U 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. 4. Click on “Browse” and Locate the backup file and click on “Open” as shown below. 

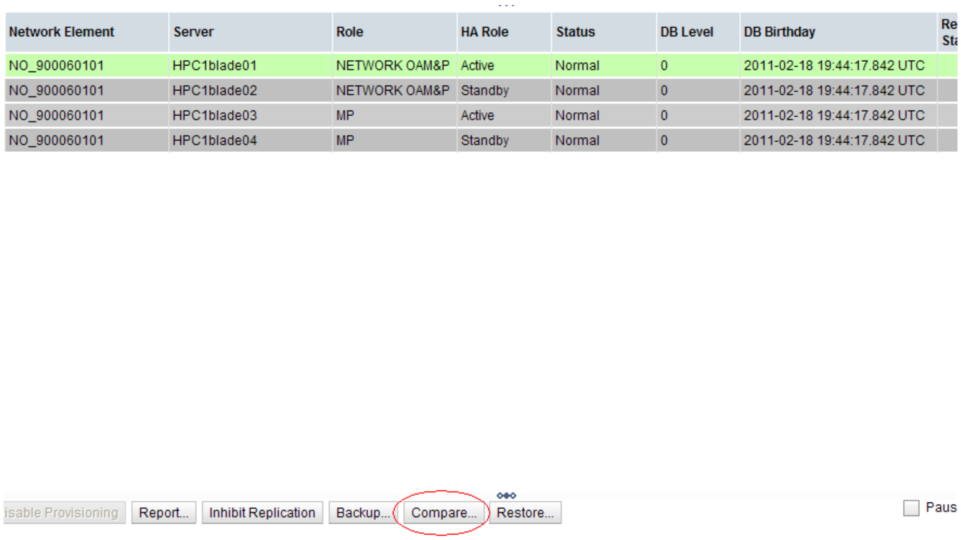
Procedure 3. Recovery Scenario 3

		 Choose file Look in: PV3 Backup.EAGLEVipelCOMProv.tgz Backup.PV3.tgz PV3_NetHawk.txt My Recent Documents Desktop My Documents My Computer My Network Places File name: Backup.PV3.tgz Files of type: All Files (*.*) Open Cancel 5. 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  Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files 2. Disable Provisioning by clicking on “Disable Provisioning” button at the bottom of the screen as shown below.  Disable Provisioning Report... Inhibit/Allow Backup... Compare... Restore... 3. A confirmation window will appear, press “OK” to disable Provisioning.  Message from webpage Disable provisioning. Are you sure? 4. The message “Warning Code 002” will appear.

Procedure 3. Recovery Scenario 3

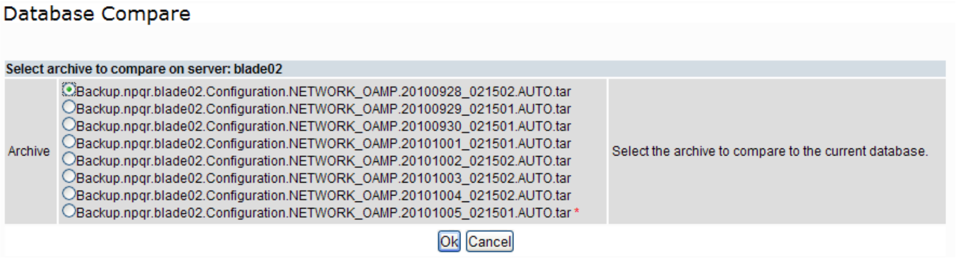
7 □ Verify the Archive Contents and Database Compatibility

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

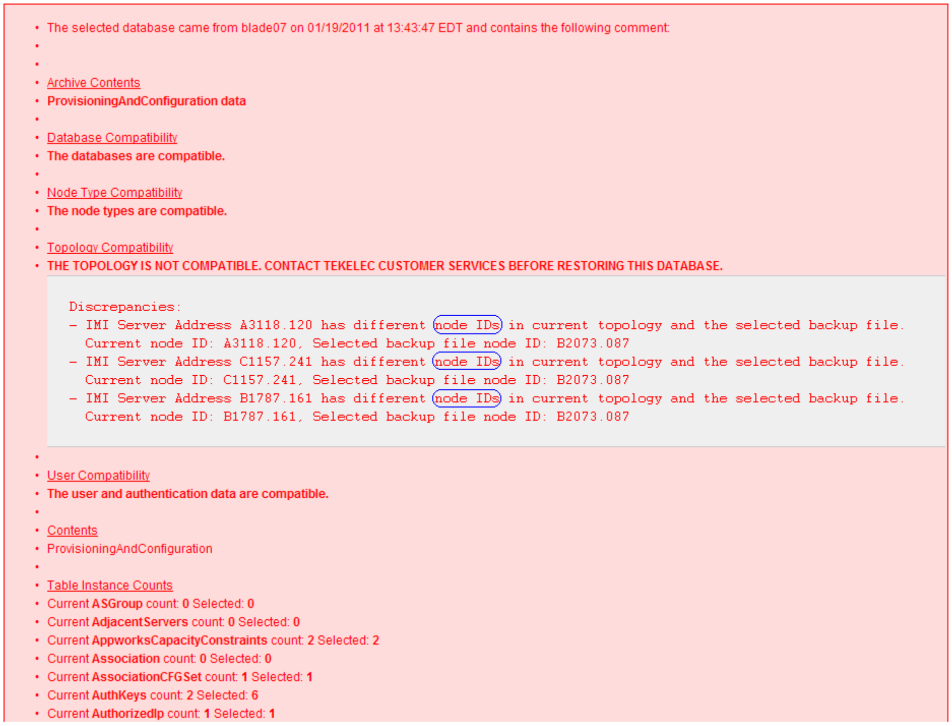
Select archive to compare on server: blade02

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

Procedure 3. Recovery Scenario 3



- 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: Provisioning and 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:

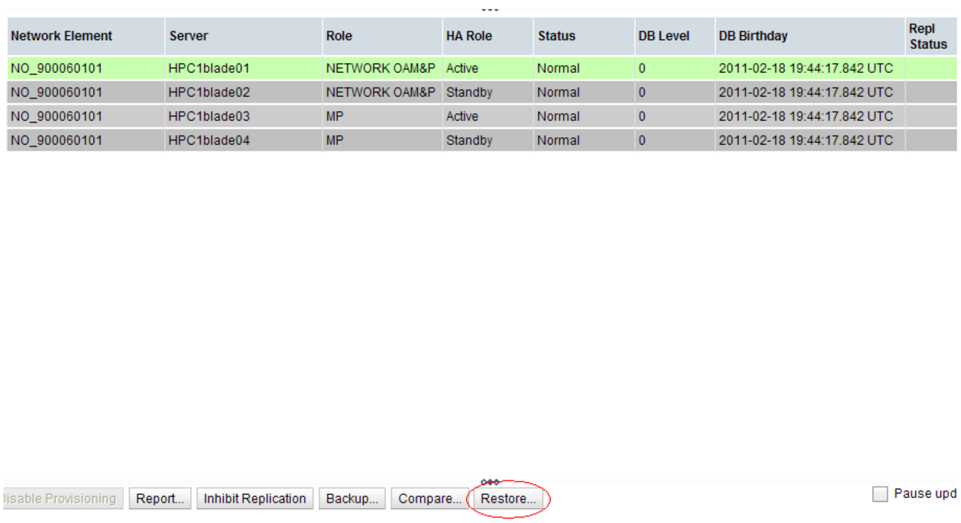
Topology Compatibility
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

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.

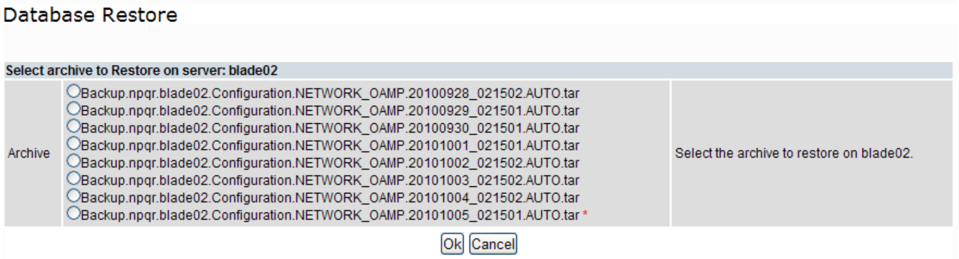
8 □ Restore the Database

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.

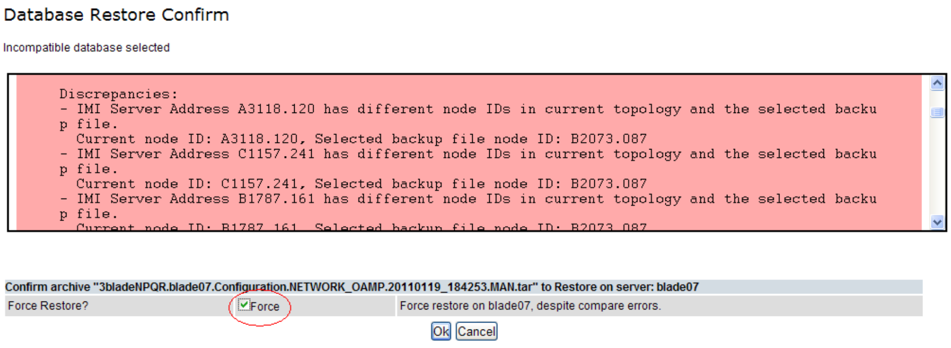


Database Restore

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

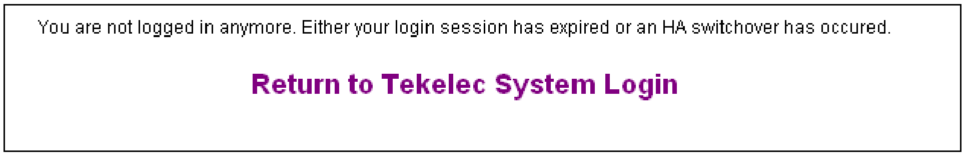
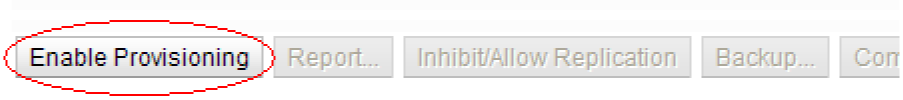
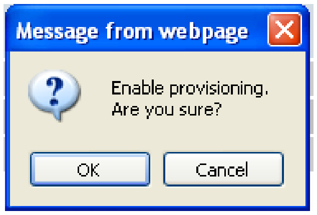
Incompatible database selected

```
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
```

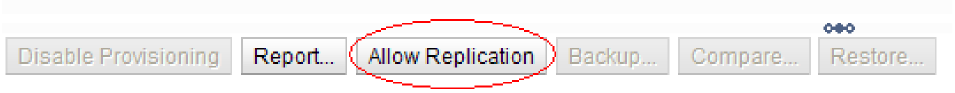
Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07		
Force Restore?	☑Force	Force restore on blade07, despite compare errors.

6. To check the status of the restore process, navigate to Main Menu->Status & Manage ->Database, the status will be displayed as shown below.

Procedure 3. Recovery Scenario 3

		 The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location. **NOTE:** After the restore has started, the user will be logged out of 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?

Procedure 3. Recovery Scenario 3

10 □	Restore /etc/hosts file of active NO	**Release 5.X:** From the recovered NO server command line, execute: `# AppWorks AppWorks_AppWorks updateServerAliases <NO Host Name>` **Release 4.X:** 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)
11 □	Recover standby NO server.	Recover the standby NO server: 1. Install the second NO server by executing Reference [5], Procedure "Configure the Second NOAMP Server, steps 1, 4, 5 and 6". 2. If you are using Netbackup, execute Procedure 35 from [5] or Procedure 13 from [7], "Install Netbackup Client
12 □	Recover SO servers.	Recover the remaining SO servers (standby, spare) by repeating the following step for each SO Server: 1. Install the second SO server by executing Reference [5] for DSR 4.x or reference [7] for DSR 5.x, Procedure "Configure the SOAM Servers", steps 1, 4, 5 and 6".
13 □	Recover the MP Servers (also applies to IPFE servers)	Execute the following procedures from [5] (4.X) or [7] (5.X) FOR **EACH** MP that has been recovered: 1."Configure MP Blades Servers", Steps 1, 4, 5, 6 and 7 2. (**DSR 4.X ONLY):** 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>** 3 If IPFE servers are being recovered, execute Procedure 5 of [20] for any applicable IPFE servers.
14 □	**DSR 5.X Recovery Only:** Re-Sync NTP if Necessary (Optional)	Navigate to **Status & Manage** -> **Server,** then select each server that has been recovered and click **NTP Sync**..
15 □	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.
16 □	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.: p. Active NOAMP Server q. Standby NOAMP Server r. Active MP Servers s. Standby MP Servers  Disable Provisioning Report... Allow Replication Backup... Compare... Restore... 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".

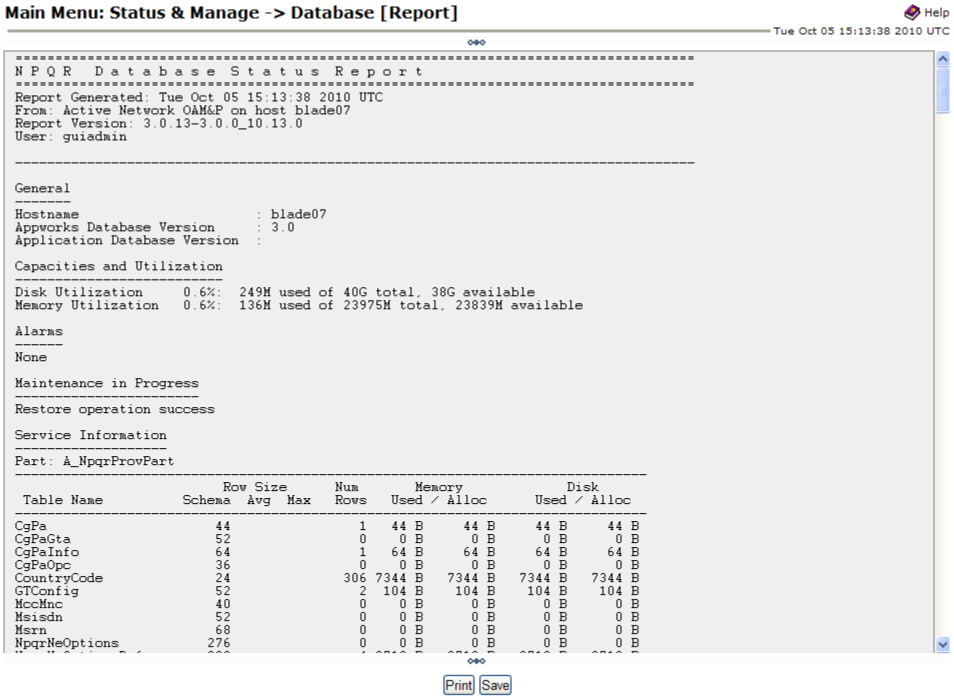
Procedure 3. Recovery Scenario 3

17 □ Remove Forced Standby

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**

18 □ 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]

Tue Oct 05 15:13:38 2010 UTC

```
=====================================================================================
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.

19 □ Optimize Comcol memory usage on recovered NO and SO (**DSR 4.X only)**

If recovering a DSR 4.x system, execute this step, otherwise skip to step 19.

For each recovered NO or SO, obtain a terminal window connection to the (NO/SO) server console via SSH or iLO. **If using SSH, use the actual IP of the server, not the VIP address.**

Execute the following on the command line. Wait until the script completes and you are returned to the command line:

```
# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage

# sleep 20

# prod.start

# pm.sanity

Sanity check OK: 01/23/13 11:42:20 within 15 secs
```

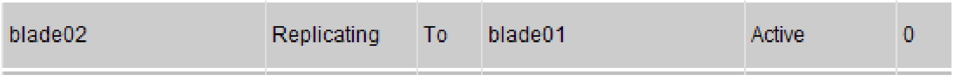
Verify that the script finished successfully by checking the exit status:

```
# echo $?
```

If anything other than "0" is printed out,. halt this procedure and contact Tekelec Support..

Repeat this step for all recovered **NO and SO servers at every site.**

Procedure 3. Recovery Scenario 3

20 □	Optimize Comcol memory usage on DA-MP**(DSR 4.X only)**	SSH to each recovered DA-MP and execute the following command. Note that this command **SHOULD NOT** be executed on SBR blades. **# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force**
21 □	Verify Replication between servers.	1. Click on Main Menu->Status and Manager->Replication 2. Verify that replication is occurring between servers Server.  blade02 Replicating To blade01 Active 0
22 □	Verify the Database states	1. Click on Main Menu->Status and Manager->Database 2. Verify that the HA Role is either "Active" or "Standby", and that the status is "Normal".
23 □	Verify the HA Status	1. Click on Main Menu->Status and Manager->HA 2. Check the row for all the MP Server 3. Verify that the HA Role is either Active or Standby.
24 □	Verify the local node info	1. Click on Main Menu->Diameter->Configuration->Local Node 2. Verify that all the local nodes are listed.
25 □	Verify the peer node info	1. Click on Main Menu->Diameter->Configuration->Peer Node 2. Verify that all the peer nodes are listed.
26 □	Verify the Connections info	1. Click on Main Menu->Diameter->Configuration->Connections 2. Verify that all the peer nodes are listed.
27 □	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.
28 □	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.
29 □	Restore GUI Usernames and passwords	If applicable, Execute steps in Section 6 to recover the user and group information restored.
30 □	Backup and archive all the databases from the recovered system	Execute Appendix A back up the Configuration databases: Disaster Recovery Procedure is Complete
31 □	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

5.1.4 Recovery Scenario 4 (Partial Server Outage with one NO Server and one SO Server Intact)

For a partial outage with an NO server and an SO server intact and available, only base recovery of hardware and software is needed. The intact NO and SO servers are 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 4. 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 SO and MP servers by recovering base hardware and software.
  - **Recover** the base **hardware**.
  - **Recover** the **software**.
  - The database in intact at the active NO server and does not require restoration at the SO and MP servers.
- Re-apply signaling networks configuration if the failed blade is an MP.

Follow procedure below for detailed steps.

Procedure 4. Recovery Scenario 4

S T E P #	This procedure performs recovery if at least 1 NO server is intact and available and 1 SO server is intact and available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Note: If any errors are encountered during the execution of this procedure, refer to the list of known issues in Appendix E before contacting Tekelec Customer Support 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. **Note:** If necessary, Refer to [8] *PM&C Disaster Recover* on instructions how to recover a PM&C Server. If both NO servers are intact and available, skip this step and go to Step 2. If the standby NO server has failed: 1. 1 From the NO VIP GUI, set the server HA state to "Forced Standby" by navigating to Main Menu->HA, then clicking on Edit and setting the "Max Allowed HA Role" to Standby for the NO in question and pressing OK. 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. Remove the failed HP c-Class Blade and install the replacement into the enclosure. 4. Configure and verify the BIOS on the Blade. Execute procedure "Confirm/Update Blade Server BIOS Settings" from reference [5] for DSR 4.x or reference [6] for DSR 5.x. 5. Execute Procedure "Configure iLO password for Blades' Administrator Account" from [5] to setup the root password on the newly installed blade. For RMS based servers, execute Appendix I from [3] to configure all iLO settings, including the iLO password. 6. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details. 7. Execute procedure "Install TVOE on Server Blades" from reference [5] for DSR 4.x or reference [7] for DSR 5.x. (Blade-based NOAMPs only) 8. Execute procedure "Configure TVOE on Server Blades" from reference [5] for DSR 4.x or reference [7] for DSR 5.x. (Blade-based NOAMPs only). 9. Execute procedure "Continue TVOE Configuration on First RMS Server" from reference [5] for DSR 4.x or reference [6] for DSR 5.x. (RMS based NOAMPs only) 10. Execute procedure "Configure TOVE on Additional RMS Server(s)" from reference [5] for DSR 4.x or reference [6] for DSR 5.x. (RMS based NOAMPs only) 11. Execute procedure "Create NOAMP Guest VMs" from reference [5] for DSR 4.x or reference [7] for DSR 5.x. 12. 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 . 13. IPM The standby NO using procedure "IPM Blades and VMs" from [5]. or [7] 14. Install the application on the Standby NO using procedure "Install the Application Software on the Blades" from [5] for DSR 4.x or reference [7] for DSR 5.x. 15. Configure the newly installed application by executing procedure "Configure the Second NOAMP Server, from [5] 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". 18. From the NO VIP GUI, set the server HA state to "Forced Stand by" by navigating to Main Menu->HA, then clicking on Edit and setting the "Max Allowed HA Role" to Active for the NO server in question and pressing OK.

Procedure 4. Recovery Scenario 4

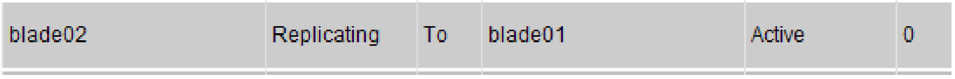
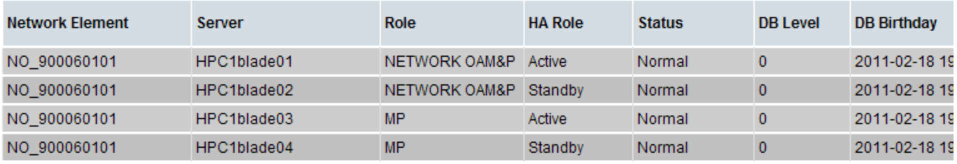
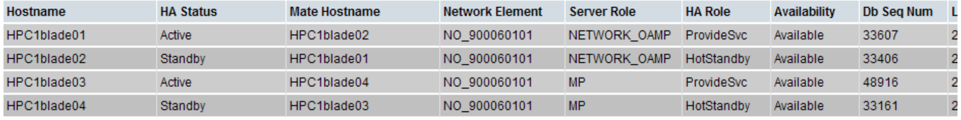
2 □	Recover SO servers (if needed).	Recover the SO server(s) (if needed) by recovering base hardware and software. If both SO servers are intact and available, skip this step and go to Step 3. Execute the following for any SO server that has failed: 1. Gather the documents and required materials listed in Section 3.1. 2. From the NO VIP GUI, set the server HA state to “Forced Standby” by navigating to Main Menu->HA, then clicking on Edit and setting the “Max Allowed HA Role” to Standby for the SO in question and pressing OK. 3. From the NO VIP GUI, Inhibit replication to the standby SO by navigating to Main Menu->Status & Manage-> Database, then selecting the SO in question and clicking on “Inhibit Replication”. 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] for DSR 4.x or reference [6] for DSR 5.x. 6. Execute Procedure “Configure iLO password for Blades’ Administrator Account” from [5] for DSR 4.x or [6] for DSR 5.X 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] for DSR 4.x or reference [6] for DSR 5.x. 9.Execute procedure “Configure TVOE on Server Blades” from reference [5] for DSR 4.x or reference [6] for DSR 5.x. 10.Execute procedure “Create SOAM Guest VMs” from reference [5] for DSR 4.x or reference [7] for DSR 5.x. 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 SO using procedure “IPM Blades and VMs” from [5] for DSR 4.x or reference [7] for DSR 5.x. 13. Install the application on the SO using procedure “Install the Application Software on the Blades” from [5]. 14. Configure the newly installed application by executing procedure “Configure the SOAM Server, from [5] for DSR 4.x or reference [7] for DSR 5.x steps 1, 2, 4, 5 and 6. 15. Re-enable Replication to the restored SO by navigating to Main Menu->Status & Manage-> Database, then selecting the SO in question and clicking on “Allow Replication”. 16. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered server and Clicking on “Restart”. 17. . From the NO VIP GUI, set the server HA state to “Forced Stand by” by navigating to Main Menu->HA, then clicking on Edit and setting the “Max Allowed HA Role” to Active for the SO in question and pressing OK.

Procedure 4. Recovery Scenario 4

3 □	Recover MP servers (if needed).	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] for DSR 4.x or reference [6] for DSR 5.x. (Note: If the blade has no OS installed yet, use the OA GUI to reboot the blade) 4. Execute Procedure "Configure iLO password for Blades' Administrator Account" from [5] for DSR 4.X or [6] for DSR 5.X to setup the root password on the newly installed blade. 5. IPM The failed MP(s) using procedure "IPM Blades and VMs" from [5] for DSR 4.x or reference [7] for DSR 5.x. 6. Install the application on the failed MP(s) using procedure "Install the Application Software on the Blades" from [5] for DSR 4.x or reference [7] for DSR 5.x. 7. Execute the following procedures from [5] for DSR 4.x or reference [7] for DSR 5.x "Configure MP Blades Servers", Steps 1, 4, 5-9. If using [7] for DSR 5.X, skip step 4. 8. 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". 9. (**DSR 4.X only)** Reapply the signaling Networking Configuration by running the following command from the active NO command line: **/usr/TKLC/appworks/bin/syncApplConfig <Recovered_MP_Hostame>** 10. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered servers and Clicking on "Restart". 11. If IPFE servers are being recovered, execute Procedure 5 of [20] for any applicable IPFE servers.
4 □	Remove Forced Standby	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**

5
□
	Optimize Comcol memory usage on recovered NO and SO	If recovering a DSR 4.x system, execute this step, otherwise skip to step 7.
		For each recovered NO or SO, obtain a terminal window connection to the (NO/SO) server console via SSH or iLO. **If using SSH, use the actual IP of the server, not the VIP address.**
		Execute the following on the command line. Wait until the script completes and you are returned to the command line:
		`# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage`
		`# sleep 20`
		`# prod.start`
		`# pm.sanity`
		`Sanity check OK: 01/23/13 11:42:20 within 15 secs`
		Verify that the script finished successfully by checking the exit status:
		`# echo $?`
		If anything other than "0" is printed out,. halt this procedure and contact Tekelec Support..
		Repeat this step for all recovered **NO and SO servers at every site.**

Procedure 4. Recovery Scenario 4

<table>
<tr><td>6
□</td><td>Optimize Comcol memory usage on DA-MP (<b>Execute for DSR 4.X ONLY)</b></td><td>SSH to each recovered DA-MP and execute the following command. Note that this command <b>SHOULD NOT</b> be executed on SBR blades.
<code># /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force</code></td></tr>
<tr><td>7
□</td><td>Verify Replication between servers.</td><td>1. Click on Main Menu->Status and Manager->Replication
2. Verify that replication is occurring between servers Server.

<table><tr><td>blade02</td><td>Replicating</td><td>To</td><td>blade01</td><td>Active</td><td>0</td></tr></table></td></tr>
<tr><td>8
□</td><td>Verify the Database state of the newly restored blade</td><td>1. Click on Main Menu->Status and Manager->Database
2. Verify that the HA Role is either “Active” or “Standby”, and that the status is “Normal” as shown below

<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>HA Role</th><th>Status</th><th>DB Level</th><th>DB Birthday</th></tr>
<tr><td>NO_900060101</td><td>HPC1blade01</td><td>NETWORK OAM&P</td><td>Active</td><td>Normal</td><td>0</td><td>2011-02-18 19</td></tr>
<tr><td>NO_900060101</td><td>HPC1blade02</td><td>NETWORK OAM&P</td><td>Standby</td><td>Normal</td><td>0</td><td>2011-02-18 19</td></tr>
<tr><td>NO_900060101</td><td>HPC1blade03</td><td>MP</td><td>Active</td><td>Normal</td><td>0</td><td>2011-02-18 19</td></tr>
<tr><td>NO_900060101</td><td>HPC1blade04</td><td>MP</td><td>Standby</td><td>Normal</td><td>0</td><td>2011-02-18 19</td></tr>
</table></td></tr>
<tr><td>9
□</td><td>Verify the HA Status</td><td>1. Click on Main Menu->Status and Manager->HA
2. Check the row for all the MP Server
3. Verify that the HA status is either Active of Standby as shown below.

<table>
<tr><th>Hostname</th><th>HA Status</th><th>Mate Hostname</th><th>Network Element</th><th>Server Role</th><th>HA Role</th><th>Availability</th><th>Db Seq Num</th><th>L</th></tr>
<tr><td>HPC1blade01</td><td>Active</td><td>HPC1blade02</td><td>NO_900060101</td><td>NETWORK_OAMP</td><td>ProvideSvc</td><td>Available</td><td>33607</td><td>2</td></tr>
<tr><td>HPC1blade02</td><td>Standby</td><td>HPC1blade01</td><td>NO_900060101</td><td>NETWORK_OAMP</td><td>HotStandby</td><td>Available</td><td>33406</td><td>2</td></tr>
<tr><td>HPC1blade03</td><td>Active</td><td>HPC1blade04</td><td>NO_900060101</td><td>MP</td><td>ProvideSvc</td><td>Available</td><td>48916</td><td>2</td></tr>
<tr><td>HPC1blade04</td><td>Standby</td><td>HPC1blade03</td><td>NO_900060101</td><td>MP</td><td>HotStandby</td><td>Available</td><td>33161</td><td>2</td></tr>
</table></td></tr>
<tr><td>10
□</td><td>Verify the local node info</td><td>1. Click on Main Menu->Diameter->Configuration->Local Node
2. Verify that all the local nodes are listed.</td></tr>
<tr><td>11
□</td><td>Re-install NetBackup (Optional)</td><td>1. If NetBackup was previously installed on the system, follow the procedure in [5], Appendix K to reinstall it.</td></tr>
<tr><td>12
□</td><td>Verify the peer node info</td><td>1. Click on Main Menu->Diameter->Configuration->Peer Node
2. Verify that all the peer nodes are listed.</td></tr>
<tr><td>13
□</td><td>Verify the Connections info</td><td>1. Click on Main Menu->Diameter->Configuration->Connections
2. Verify that all the peer nodes are listed.</td></tr>
<tr><td>14
□</td><td>Re-enable connections if needed</td><td>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.</td></tr>
</table>

Procedure 4. Recovery Scenario 4

15 □	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. Note: If alarm “10012: The responder for a monitored table failed to respond to a table change” is raised, the oampAgent needs to be restarted. ssh as root to each server that has that alarm and execute the following: # **pm.set off oampAgent** # **pm.set on oampAgent**
16 □	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

5.1.5 Recovery Scenario 5 (Both NO Servers failed with DR NO available)

For a partial outage with both NO servers failed but a DR NO available, the DR NO is switched from secondary to primary then recover the failed NO 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 4. The major activities are summarized as follows:

- Switch DR NO from secondary to primary
- Recover the failed NO servers by recovering base hardware and software.
    - **Recover** the base **hardware**.
    - **Recover** the **software**.
    - The database is intact at the newly active NO server and does not require restoration.
- If applicable, recover any failed SO and MP servers by recovering base hardware and software.
    - **Recover** the base **hardware**.
    - **Recover** the **software**.
    - The database in intact at the active NO server and does not require restoration at the SO and MP servers.
- Re-apply signaling networks configuration if the failed blade is an MP.

Follow procedure below for detailed steps.

Procedure 5. Recovery Scenario 5

STEP #	This procedure performs recovery if both NO servers have failed but a DR NO is available Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Note: If any errors are encountered during the execution of this procedure, refer to the list of known issues in Appendix E before contacting Tekelec Customer Support Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	
1 □	Switch DR NO to Primary	Execute Appendix C: Switching a DR Site to Primary to have the DR NO become active.
2 □	Recover System	If Both SO servers have failed, execute Recovery Scenario 2 (Procedure 2), otherwise execute procedure 4 to recover the system.
3 □	Switch NO back to Secondary	Once the system have been recovered: execute Appendix D: Returning a Recovered Site to Primary to have the recovered NO become primary again.

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.

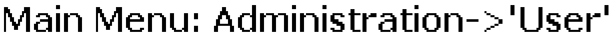
Before restoration,

- 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.



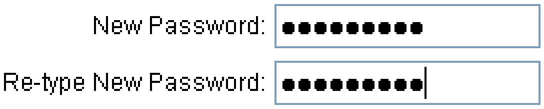
Main Menu: Administration->'User'

(Note: **for** DSR 5.X, this path is **Main Menu: Administration->Access Control->Users**)

2. Select the user.

3. Click the Change Password button.

4. Enter a new password.



New Password: ●●●●●●●●●●

Re-type New Password: ●●●●●●●●●●

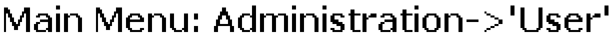
5. Click the Continue button.

6.1.2 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.

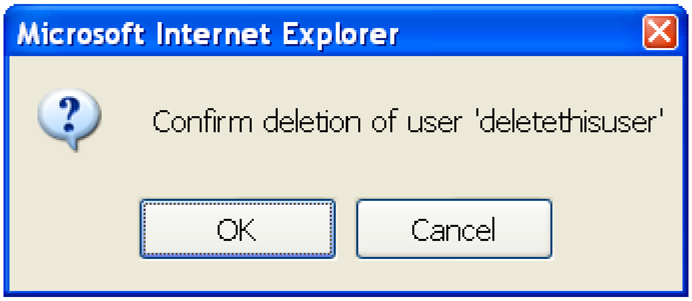
1. Navagate to the user administration screen.



Main Menu: Administration->'User'

(Note: **for** DSR 5.X, this path is **Main Menu: Administration->Access Control->Users**)

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



Confirm deletion of user 'deletethisuser'

6.2 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.

6.3 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,

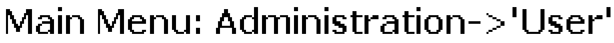
- Verify that you have access to a user with administrator permissions that is not affected.

- 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

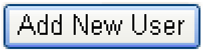
- Log in and re-create each of the affected users using the information recorded above

1. Navagate to the user administration screen.

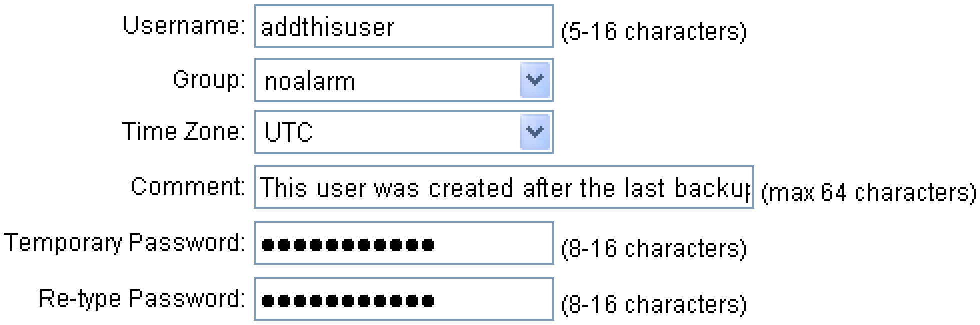


Main Menu: Administration->'User'

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 backu (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 4.x/5.x Database Backup

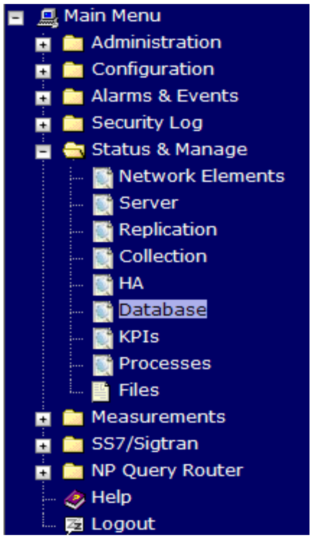
Procedure 6: DSR 4.x/5.x Database Backup

<table>
<tr><td><b>S
T
E
P
#</b></td><td colspan="2">The intent of this procedure is to backup the provision and configuration information from an NO or SO server 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 4.x "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><b>1.</b></td><td><b>Login into NO (or SO) XMI VIP IP Address</b></td><td>Login using the "guiadmin" credentials.</td></tr>
</table>

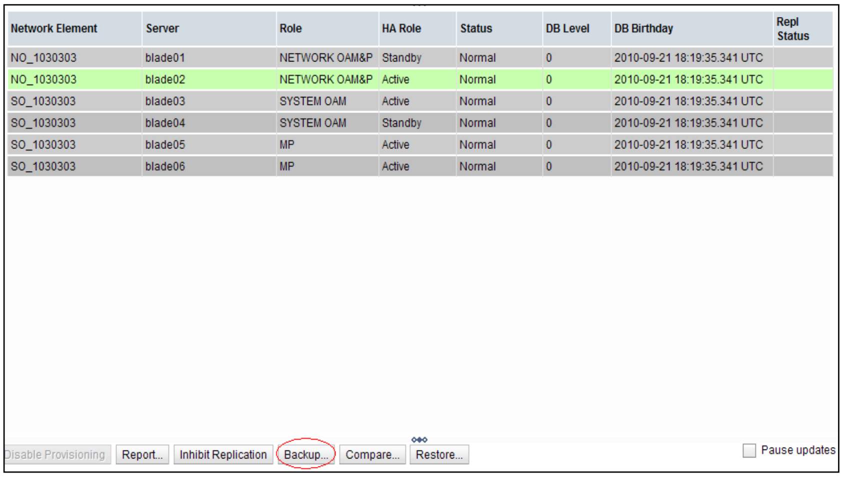
Procedure 6: DSR 4.x/5.x Database Backup

2. **Backup 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 :



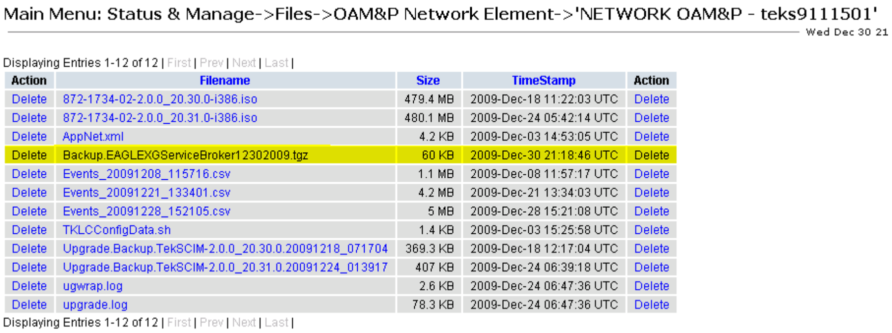
Network Element	Server	Role	HA Role	Status	DB Level	DB Birthday	Repl Status
NO_1030303	blade01	NETWORK OAM&P	Standby	Normal	0	2010-09-21 18:19:35.341 UTC	
NO_1030303	blade02	NETWORK OAM&P	Active	Normal	0	2010-09-21 18:19:35.341 UTC	
SO_1030303	blade03	SYSTEM OAM	Active	Normal	0	2010-09-21 18:19:35.341 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 is checked. Then enter a filename for the backup and press “OK”.

Procedure 6: DSR 4.x/5.x Database Backup

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

1. Browse to Main Menu-> Status & Manage->Files
2. Select the Active NO (or SO) 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 |

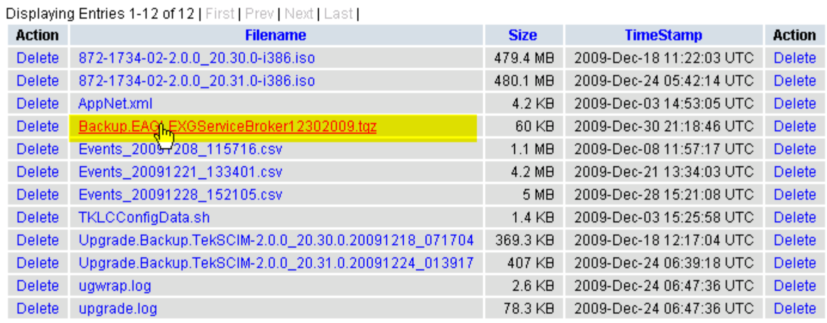
Action	Filename	Size	TimeStamp	Action
Delete	872-1734-02-2.0.0_20.30.0-i386.iso	479.4 MB	2009-Dec-18 11:22:03 UTC	Delete
Delete	872-1734-02-2.0.0_20.31.0-i386.iso	480.1 MB	2009-Dec-24 05:42:14 UTC	Delete
Delete	AppNet.xml	4.2 KB	2009-Dec-03 14:53:05 UTC	Delete
Delete	Backup.EAGLEXGServiceBroker12302009.tgz	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 configuration back up file as shown above.

Procedure 6: DSR 4.x/5.x Database Backup

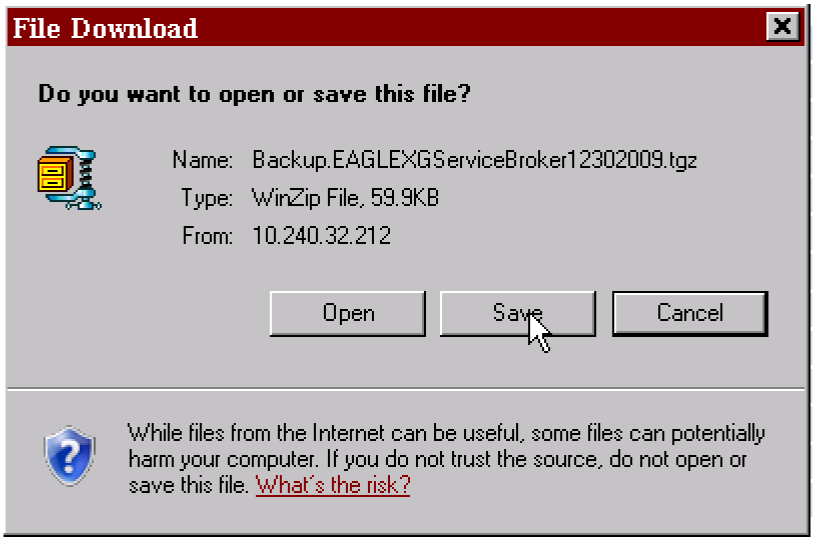
4. □	**Download the file to local machine.**	**1. Click on the file link as shown below and click on the download button**



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:



File Download

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. □	**Upload the image to secure location for future disaster recovery of entire system.**	Transfer the backed up image saved in the previous step to a secure location where the Server Backup files are fetched in case of system disaster recovery.
6. □	**Backup Active SO**	For a 3-tier system, repeat Steps 2 through 5 to backup the Active SO, otherwise the database backup of the DSR 4.x/5.x complete.

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

Procedure 7: Recovering a failed PM&C Server

S T E P #	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 [8] *PM&C Disaster Recover* on instructions how to recover a PM&C Server.

Procedure 8: Recovering a failed Aggregation Switch (Cisco 4948E / 4948E-F)

S T E P #	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 ▪ IP address and hostname of the failed switch ▪ Rack Mount position of the failed 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.		1. Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: **sudo ssh-keygen -R <4948_switch_ip>** **2.** 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 custom for this installation. These will either be stored on the PM&C in a designation location, or can be obtained from the NAPD.

Procedure 9: Recovering a failed Enclosure Switch (Cisco 3020)

<table>
<tr><td>S
T
E
P
#</td><td colspan="2">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
▪ IP address and hostname of the failed switch
▪ Interconnect Bay position of the enclosure 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.</td></tr>
<tr><td>1.</td><td></td><td>1. Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:
sudo ssh-keygen -R <enclosure_switch_ip>
2. Refer to [4], procedure "**Reconfigure a failed 3020 switch(netConfig)**", to replace a failed Enclosure switch. You will need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These will either be stored on the PM&C in a designation location, or can be obtained from the NAPD.</td></tr>
</table>

Procedure 10: Recovering a failed Enclosure Switch (HP 6120XG)

<table>
<tr><td>S
T
E
P
#</td><td>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
▪ IP address and hostname of the failed switch
▪ Interconnect Bay position of the enclosure switch
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.</td></tr>
</table>

Procedure 10: Recovering a failed Enclosure Switch (HP 6120XG)

1.		1. Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: **sudo ssh-keygen -R <enclosure_switch_ip>** 2. Refer to [4], procedure “**Reconfigure a failed HP 6120XG switch (netConfig)**”, to replace a failed Enclosure switch. You will need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These will either be stored on the PM&C in a designation location, or can be obtained from the NAPD.

Procedure 11: Recovering a failed Enclosure Switch (HP 6125XG)

S T E P #	The intent of this procedure is to recover a failed Enclosure (6125XG) 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.	
2.		1. Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: **sudo ssh-keygen -R <enclosure_switch_ip>** 2. Refer to [4], procedure “**Reconfigure a failed HP 6125XG switch (netConfig)**”, to replace a failed Enclosure switch. You will need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These will either be stored on the PM&C in a designation location, or can be obtained from the NAPD.

Procedure 12: 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.

Procedure 12: Recovering a failed Enclosure OA

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

Appendix C. Switching a DR Site to Primary

Upon the loss of a Primary DSR NO Site, the DR NO Site should become primary. The following steps are used to enable such switchover.

Preconditions:

- User cannot access the primary DSR
- User still can access the DR DSR
- Provisioning clients are disconnected from the primary DSR
- Provisioning has stopped

Recovery Steps

In order to quickly make DSR GUI accessible and provisioning to continue, DR DSR servers are activated and made to serve as primary DSR via following steps.

1 □	Disable the application on DR DSR servers.	This step ensures that when the DR DSR assumes Primary status in a controlled fashion. Disabling the application inhibits provisioning and can be started after successful validation. 1. Login to DR DSR GUI as one of the admin user. 2. Select [Main Menu: Status & Manage → Server] screen. 3. Select the row that has active DR DSR server. It highlights ‘Stop’ button at the bottom. 4. Click the ‘Stop’ button and then click the ‘OK’ button. At this time, HA switch over causes an automatic logout. 5. Login to DR DSR GUI as one of the admin user. 6. Repeat step 3 to 4 for new active DR DSR server. 7. Verify that ‘PROC’ column on both DR DSR servers show ‘Man’ indicating that application is manually stopped.
2 □	SSH to physical IP address of the designated primary DR DSR as root and make it primary	1. Login via SSH to the physical IP of the chosen primary DR DSR server as root user. 2. Execute the command top.setPrimary This step makes the DR DSR take over as the Primary. 3. System generates several replication and collection alarms as replication/collection links to/from former Primary DSR servers becomes inactive.
3 □	Verify replication	1. Monitor [Main Menu: Status & Manage → Server] screen at new-Primary DSR. 2. It may take several minutes for replication, afterward the DB and Reporting Status columns should show ‘Normal.’
4 □	Re-enable the application on the now-Primary DSR using the Active new-Primary DSR GUI.	1. Login to new-Primary DSR GUI as one of the admin user. 2. Select [Main Menu: Status & Manage → Server] screen. 3. Select the row that has the active new-Primary DSR server. This action highlights the ‘Restart’ button at the bottom. 4. Click the ‘Restart’ button and then click the ‘OK’ button. 5. Verify that ‘PROC’ column now shows ‘Norm’. 6. Repeat step 3 to 5 for standby new-Primary DSR server. Provisioning connections can now resume to the VIP of the new-Primary DSR.

5 □	Decrease the durability admin status and then reconfigure and reconnect the customer's provisioning clients.	1. Lower the durability admin status to (NO pair) to exclude former-Primary DSR servers from the provisioning database durability. A value greater than 2 must be adjusted downward. a. Login to new DSR GUI as admin user b. Select [Main Menu: Administration → General Options] c. Set *durableAdminState* to 0 (NO pair) d. Click the 'OK' button 2. Have customer reconfigure provisioning clients to connect to XMI VIP of the newly activated DSR servers. 3. Verify that provisioning from clients have started. a. Select [Main Menu: DSR → Maintenance → Command Log] b. Check that new commands have been executed
6 □	Bring former-Primary DSR back to service (Optional).	1. Determine what has happened to former-Primary DSR site. DSR frame defective__________ DSR servers defective _________ Networking outage ________ Switch defective _________ 2. Based on the above disaster recovery scenario, execute procedure from this document to return the former-Primary DSR servers and site back to service.
7 □	Convert former Primary DSR servers to new DR DSR (Optional)	1. SSH to active former-Primary DSR server as root. 2. Execute the command top.setSecondary This step allows the formerly Primary DSR to become the DR DSR. 3. Monitor [Main Menu: Status & Manage → Server] screen at new DR DSR GUI. 4. It may take several minutes for replication, afterward the DB and Reporting Status columns should show 'Normal.'
8 □	Set durability admin status to include DR DSR (Optional)	1. If you reduced the durability status in step 5, raise durability admin status to its former value (NO + DRNO) . a. Login to new primary DSR GUI as admin user b. Select [Main Menu: Administration → General Options] c. Set *durableAdminState* to 3(NO DRNO) d. Click the 'OK' button 2. Now new DR DSR servers are part of provisioning database durability.

Appendix D. Returning a Recovered Site to Primary

Once a failed site is recovered, the customer might choose to return it to primary state while returning the current active site to its original DR State. The following steps are used to enable such switchover.

Preconditions:

- Failed Primary DSR site recovered

Recovery Steps

In order to quickly make DSR GUI accessible and provisioning to continue, DR DSR servers are activated and made to serve as primary DSR via following steps.

1 □	Disable the application on currently Active DSR servers.	Disabling the application inhibits provisioning and can be started after successful validation. 1. Login to Active DSR GUI as one of the admin user. 2. Select [Main Menu: Status & Manage → Server] screen. 3. Select the row that has active DSR server. It highlights 'Stop' button at the bottom. 4. Click the 'Stop' button and then click the 'OK' button. At this time, HA switch over causes an automatic logout. 5. Login to DR DSR GUI as one of the admin user. 6. Repeat step 3 to 4 for new active DR DSR server. 7. Verify that 'PROC' column on both DR DSR servers show 'Man' indicating that application is manually stopped.
2 □	Convert former Primary DSR servers to new DR DSR	1. SSH to VIP of active former-Primary DSR server as root. 2. Execute the command top.setSecondary This step allows the formerly Primary DSR to become the DR DSR. 3. Monitor [Main Menu: Status & Manage → Server] screen at new DR DSR GUI. 4. It may take several minutes for replication, afterward the DB and Reporting Status columns should show 'Normal.'
3 □	Start software on newly DR Site	1. Login to new-DR DSR GUI physical IP as one of the admin user. 2. Select [Main Menu: Status & Manage → Server] screen. 3. Select the row that has the active new-DR DSR server. This action highlights the 'Restart' button at the bottom. 4. Click the 'Restart' button and then click the 'OK' button. 5. Verify that 'PROC' column now shows 'Norm'. 6. Repeat step 3 to 5 for standby new-DR DSR server.
4 □	SSH to VIP address of the to-be-primary DSR as root and make it primary	1. Login via SSH to VIP of to-be-primary DSR server as root user. 2. Execute the command top.setPrimary This step makes the DSR take over as the Primary. 3. System generates several replication and collection alarms as replication/collection links to/from former Primary DSR servers becomes inactive.

5 □	Re-enable the application on the now-Primary DSR using the Active new-Primary DSR GUI.	1. Login to new-Primary DSR GUI as one of the admin user. 2. Select [Main Menu: Status & Manage → Server] screen. 3. Select the row that has the active new-Primary DSR server. This action highlights the 'Restart' button at the bottom. 4. Click the 'Restart' button and then click the 'OK' button. 5. Verify that 'PROC' column now shows 'Norm'. 6. Repeat step 3 to 5 for standby new-Primary DSR server. Provisioning connections can now resume to the VIP of the new-Primary DSR.
6 □	Verify replication	1. Monitor [Main Menu: Status & Manage → Server] screen at new-Primary DSR. 2. It may take several minutes for replication, afterward the DB and Reporting Status columns should show 'Normal.' Note: the inetmerge process might have to be restarted if replication is taking excessive time. To restart it, ssh to the active site NO and run the following command to restart the replication process:: # **pm.kill inetmerge**
7 □	Decrease the durability admin status and then reconfigure and reconnect the customer's provisioning clients.	1. Lower the durability admin status to (NO pair) to exclude former-Primary DSR servers from the provisioning database durability. A value greater than 2 must be adjusted downward. a. Login to new DSR GUI as admin user b. Select [Main Menu: Administration → General Options] c. Set *durableAdminState* to 0 (NO pair) d. Click the 'OK' button 2. Have customer reconfigure provisioning clients to connect to XMI VIP of the newly activated DSR servers. 3. Verify that provisioning from clients have started. a. Select [Main Menu: DSR → Maintenance → Command Log] b. Check that new commands have been executed
8 □	Set durability admin status to include DR DSR (Optional)	3. If you reduced the durability status in step 5, raise durability admin status to its former value (NO + DRNO) . a. Login to new primary DSR GUI as admin user b. Select [Main Menu: Administration → General Options] c. Set *durableAdminState* to 3(NO DRNO) d. Click the 'OK' button 4. Now new DR DSR servers are part of provisioning database durability.

Appendix E. 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	222829,234357	**Release 5.X:** From the recovered NO server command line, execute: # **AppWorks AppWorks_AppWorks updateServerAliases <NO Host Name>** **Release 4.X:** 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 F. 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 ATCA Shelf level FRU is requested. The CCC may be reached using the following contact information:

Tekelec Customer Care Center

US: 1-888-367-8552