Oracle® Communications Diameter Signaling Router

RMS Productization Disaster Recovery Guide

Release 4.X/5.X

909-2267-001

June 2014

Oracle Communications Diameter Signaling Router RMS 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 4.1 RMS Productization deployment. This includes recovery of partial or a complete loss of one or both RMS servers. The audience for this document includes groups such as Software Engineering, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. The target audience does not include Tekelec customers. This document provides step-by-step instructions to execute disaster recovery. 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. ([8] for SDS and [9] chapter 6 for DIH)

Note that this document only covers the disaster recovery scenarios of DSR 4.1 RMS Productization deployments. For all other DSR deployments, refer to [10] for 3-tier deployments, and refer to [11] for 2-tier deployments.

1.2 References

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

[2] *DSR 4.1RMS Productization Networking Interconnect Technical References*, TR007187, v. 1.0 or greater, P. Mouallem, 2012

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

[4] *Platform 6.x Configuration Procedure Reference*, 909-2209-001, v. 1.0 or greater, L. Antosova et al., 2012

[5] *DSR 4.1 RMS Productization Installation*, 909-2255-001, latest version, P. Mouallem, 2013

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

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

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

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

[10] *DSR 4.x/3-tier Disaster Recovery*, 909-2246-001, latest Version, P. Mouallem, November 2012

[11] *DSR 3.0/2-tier Disaster Recovery*, 909-2225-001, latest Version, P. Mouallem, November 2012

1.3 Software Release Numbering

This procedure applies to all EAGLE XG DSR 4.1 on RMS releases.

1.4 Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DIH	Diameter Intelligent Hub
DVD	Digital Versatile Disc
FRU	Field Replaceable Unit
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
OS	Operating System (e.g. TPD)
PM&C	Platform Management & Configuration
RMS	Rack Mount Server
SDS	Subscriber Data Server
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine
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 DSR RMS Productization disaster recovery procedure falls into two basic categories

Recovery of the entire network from a total outage

- Both RMS servers failed

Recovery of one RMS server with the other RMS Server intact

- 1 RMS server with all its VMs intact
- 1 RMS server failed (including all its VMs)

Note that for Disaster Recovery of the PM&C Server and Aggregation switches, refer to Appendix B.

2.1 Complete Outage (All servers)

This is the worst case scenario where both RMS servers 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 Outage with one RMS Intact

This case assumes that one RMS Server and all its VMs is intact. The server that failed is recovered using base recovery of hardware and software. VMs are created and setup. Replication will recover the database and configuration.

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 (909-2267-001) and hardcopies of all documents in the reference list: [1] through [5].
2. Hardcopy of all site surveys performed at the initial installation and network configuration files of this customer's site. The site surveys is managed by the TAC team, and they can provide the location where the files are stored.
3. EAGLE XG DSR 4.1 backup files: electronic backup file (preferred) or hardcopy of all DSR 4.1 configuration and provisioning data. Check [7] for more details on the backup procedure.
4. Latest Network Element report: electronic file or hardcopy of Network Element report.
5. Tekelec Platform Distribution (TPD) Media (64 bits).
6. Platform Management & Configuration (PM&C) Media.
7. EAGLE XG DSR 4.1 or later Media of the target release.
8. The xml configuration files used to configure the switches, available on the PM&C Server.
9. The network element XML file used for the initial configuration.
10. The HP firmware upgrade Kit
11. NetBackup Files if they exist

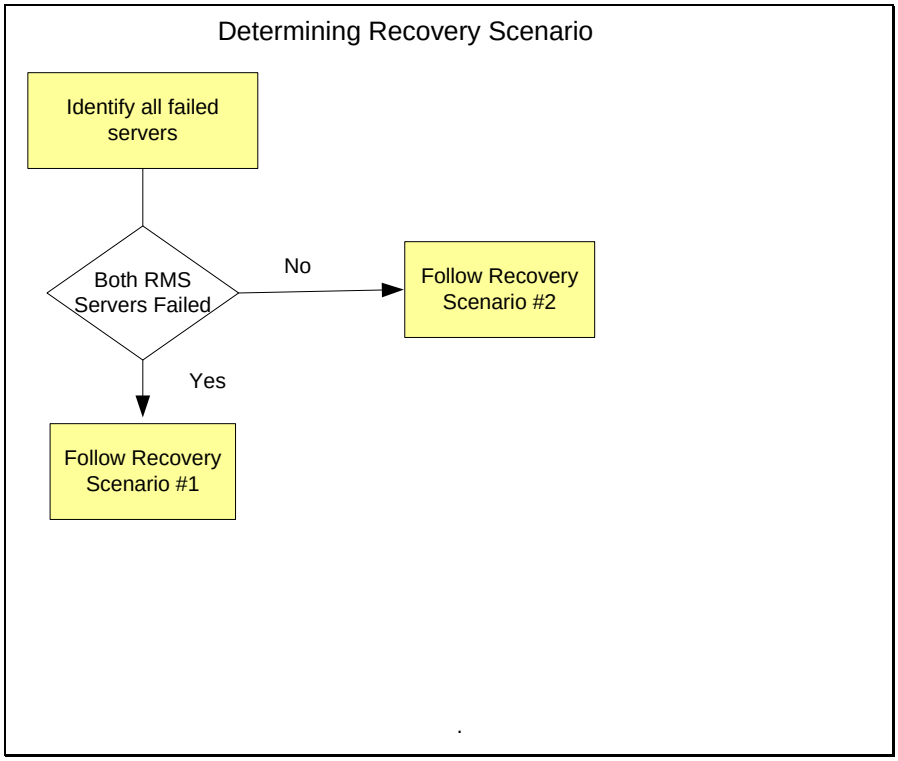
For all Disaster Recovery scenarios, we assume that the NO Database backup and the SO Database backup were performed around the same time, and that no synchronization issues exist among them.

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



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 RMS Servers completely failed (All VMs unavailable).	Execute Section 5.1.1, Procedure 1.
2	• 1 RMS server is intact and available. • 1 RMS server failed.	Execute Section 5.1.2, Procedure 2.

5 DISASTER RECOVERY PROCEDURE

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

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

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

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

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

Recovering Base Hardware

1. Hardware Recovery will be executed bv Tekelec.
2. Base Hardware Replacement must be controlled by engineer familiar with DSR 4.1 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 Outage)

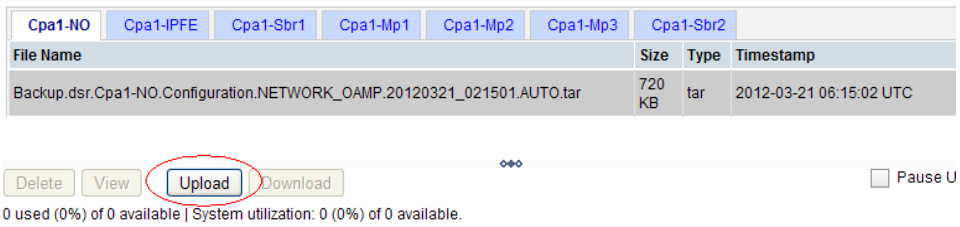
For a complete server outage, TVOE and PMAC is recovered on both RMS Servers. The VMs are re-created and configured. The database restored on one of the NO and SO servers. Database replication from the active NO server will recover the database on these servers. The major activities are summarized in 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 both RMSs.
    - Recover the base hardware. (by replacing the hardware and executing hardware configuration procedures, reference [5]).
    - Recover the Virtual Machines. (by executing procedures from reference [5])
    - Recover the software. (by executing installation procedures, reference [5])
- Recover PM&C
- Recover Active NO Guest.
    - Recover the NO database.
    - Reconfigure the application
- Recover Standby NO Guest.
    - Reconfigure the Application
- Recover all SO and MP Guest.
    - Recover the SO database.
    - Reconfigure the Application
- Restart processes and re-enable provisioning and replication.

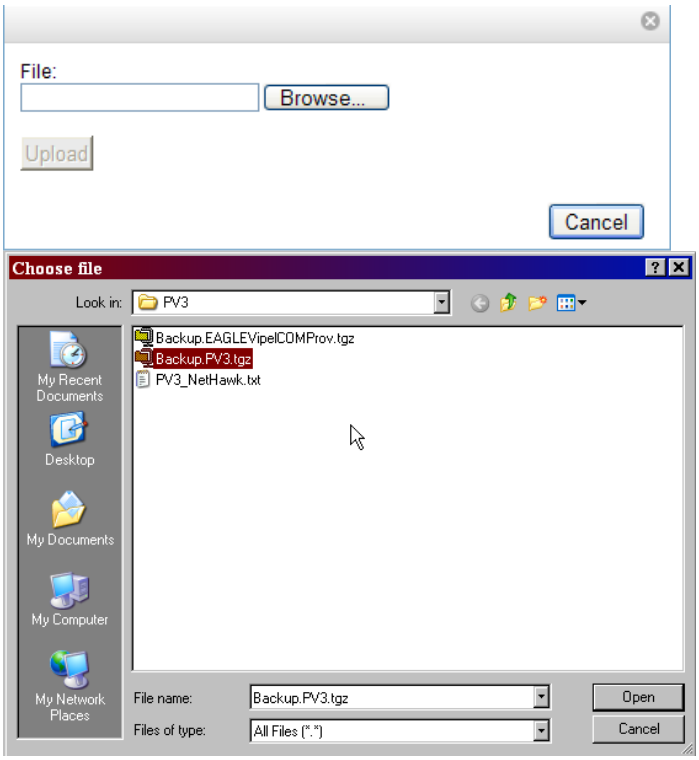
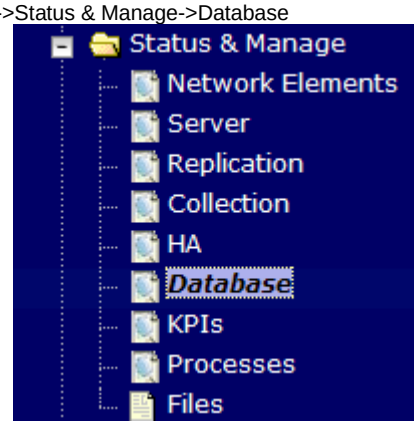
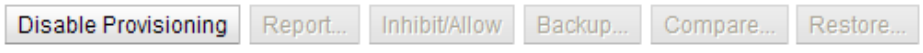
Note that any other applications DR recovery actions (SDS and DIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution (i.e. stale DB on DP servers will not receive updates until SDS-SO servers are recovered

Follow procedure below for detailed steps.

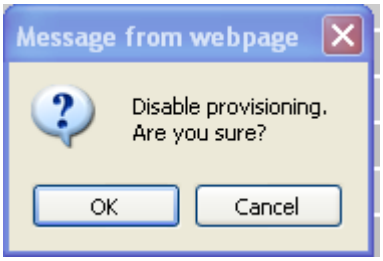
Procedure 1. Recovery Scenario 1

S T E P #		
	This procedure performs recovery if both RMS 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 Both failed servers: 1. Gather the documents and required materials listed in Section 3.1. 2. Remove the failed RMS Servers and install replacements. 3. Configure and verify the BIOS on the RMS. Execute procedure "Configure the RMS Server BIOS Settings and Update Firmware" from reference [5]. 4.Execute procedure "Install TVOE 2.0 on First RMS Server" from reference [5]. 5.Execute procedure "First RMS Configuration" from reference [5]. 6.Execute procedure 6 from Appendix B to recover the PM&C 7.Execute procedure "Install TVOE on Second RMS" from reference [5]. 8.Execute procedure "Configure TVOE on Second RMS Server" from reference [5]. 9.Execute procedure "Load ISOs onto PM&C Server" from reference [5]. 10.Execute procedure "Create NOAMP Guest VMs" from reference [5]. 11.Execute procedure "Create SOAM Guest VMs" from reference [5]. 12.Execute procedure "Create MP Guest VMs" from reference [5]. 13.If applicable, execute procedure "Create IPFE Guest VMs" from reference [5]. 14. IPM all the guests using procedure "Install the Software on the VMs" from [5].
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 4.1 database backup file. 2. From required materials list in Section 3.1; use site survey documents and Network Element report (if available), to determine network configuration data.
3 ☐	Execute EAGLE XG DSR 4.1 Installation procedures.	Execute procedures from EAGLEXG DSR 4.1 Installation User's Guide. 1. Verify the networking data for Network Elements. Use the backup copy of network configuration data and site surveys (from Step 2) 2. Install the first NO server, you will need to obtain the network element XML file from the PM&C Server: Execute installation procedures for the first NO server. See reference [5], Procedure "Configure the First NOAMP NE and Server", and "Configure the NOAMP Server Group".
4 ☐	Login into the NO XMI VIP Address	Log into the first NO GUI.
5 ☐	Upload the backed up database file from Remote location into File Management Area.	1. Browse to Main Menu->Status & Manage->Files 2. Select the Active NO Server. The following screen will appear. Click on "Upload" as shown below and select the file "NO Provisioning and Configuration:" file backed up after initial installation and provisioning. 

Procedure 1. Recovery Scenario 1

		3. Click on “Browse” and Locate the backup file and click on “Open” as shown below.  4. Click on the “Upload ” button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
6	Disable Provisioning	1. Click on Main Menu->Status & Manage->Database  2. Disable Provisioning by clicking on “Disable Provisioning” button at the bottom of the screen as shown below.  3. A confirmation window will appear, press “OK” to disable Provisioning.

Procedure 1. Recovery Scenario 1

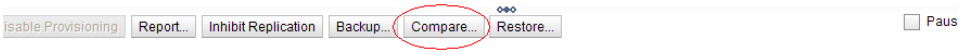


4. The message “Warning Code 002” will appear.

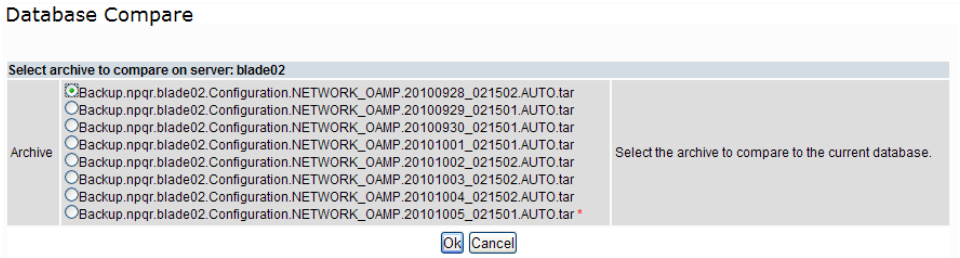
7 Verify the Archive Contents and Database Compatibility

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	

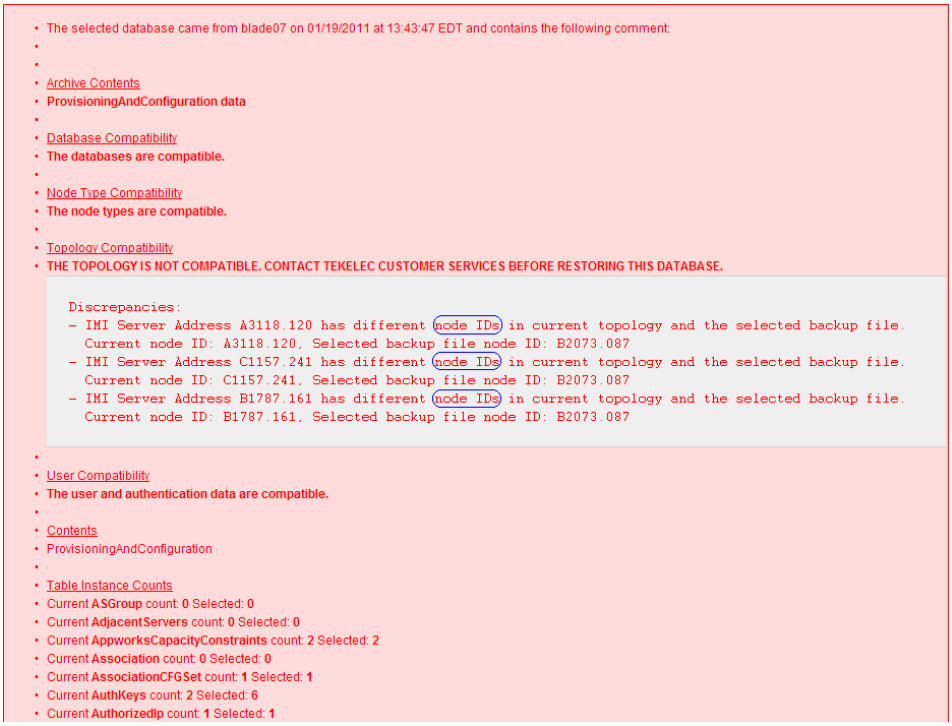


2. The following screen is displayed; click the radio button for the restored database file that was uploaded as a part of Step 2 of this procedure.



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

Procedure 1. Recovery Scenario 1



- 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:

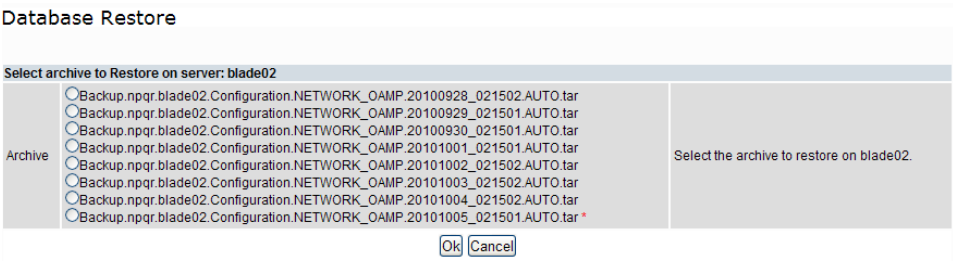
Topology Compatibility
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

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.
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

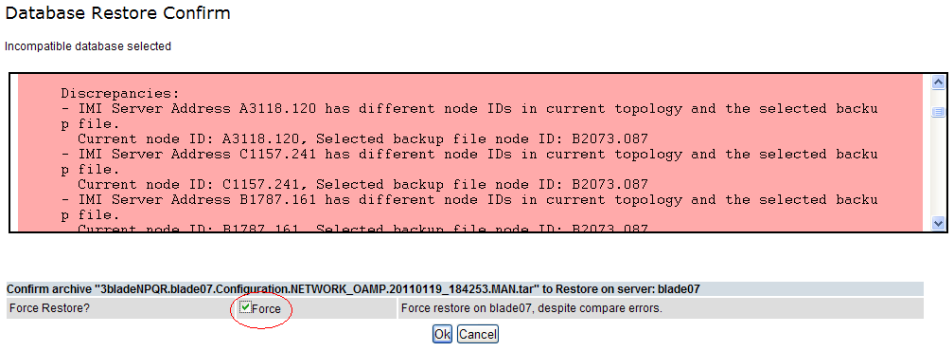
Archive	○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100930_021501.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101001_021501.AUTO.tar ○Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.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.

Ok Cancel

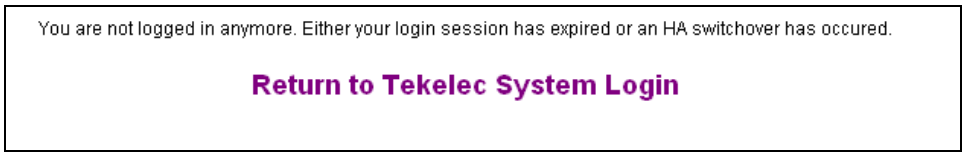
4. Click “OK” Button. The following confirmation screen will be displayed.

Procedure 1. Recovery Scenario 1

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.



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

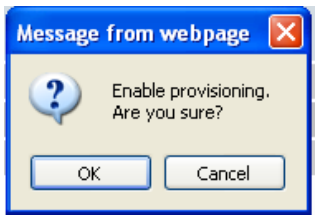


7. Log in Back into GUI VIP by clicking "Continue to this Website"
8. Login using the guiadmin login and password into the GUI
9. Wait for 5-10 minutes for the System to stabilize with the new topology.
10. Following Alarms must be ignored for NO and MP Servers until all the Servers are configured.

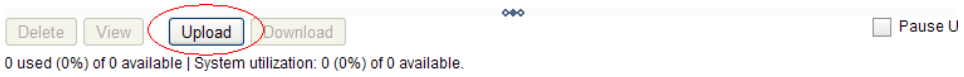
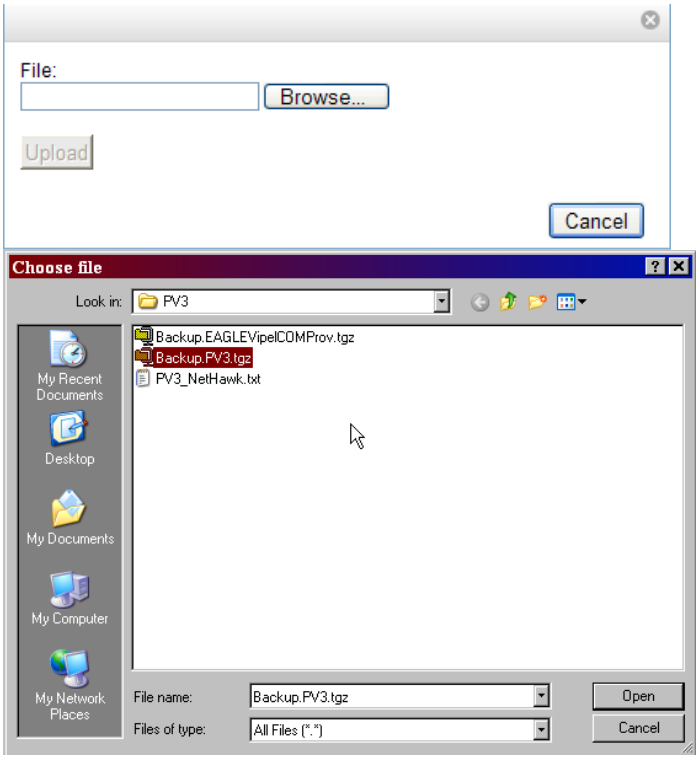
Alarms with Type Column as "REPL" , "COLL", "HA" (with mate NOAMP), "DB" (about Provisioning Manually Disabled)

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

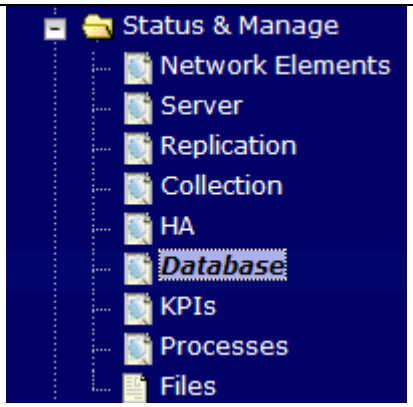
NOTE: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.

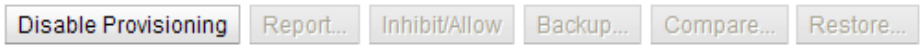
9 ☐	Re-enable Provisioning	1. Click on Main Menu->Status & Manage->Database menu item.  2. Click on the "Enable Provisioning" button. A pop-up window will appear to confirm as shown below, press OK. 

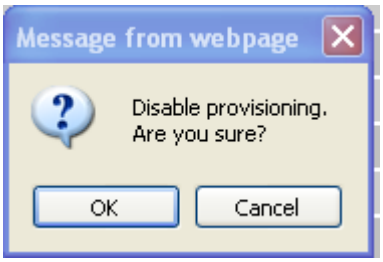
Procedure 1. Recovery Scenario 1

10 ☐	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".
11 ☐	Recover SO servers.	Recover the Active SO server: Install the SO servers by executing Reference [5], Procedure "Configure the SOAM Servers, steps 1, 4, 5, 6 and 7".
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.  3. Click on "Browse" and Locate the backup file and click on "Open" as shown below.  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

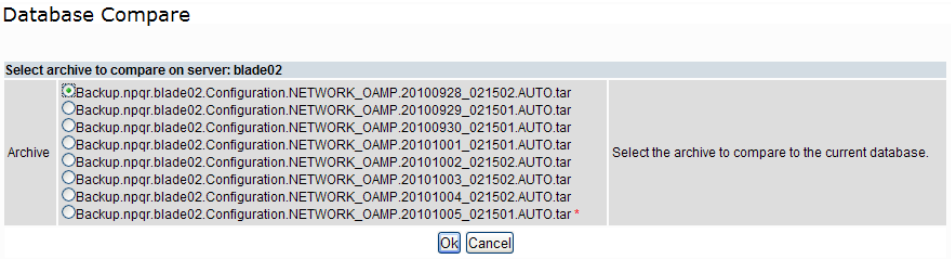
Procedure 1. Recovery Scenario 1

<table>
<tr><td></td><td></td><td>


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


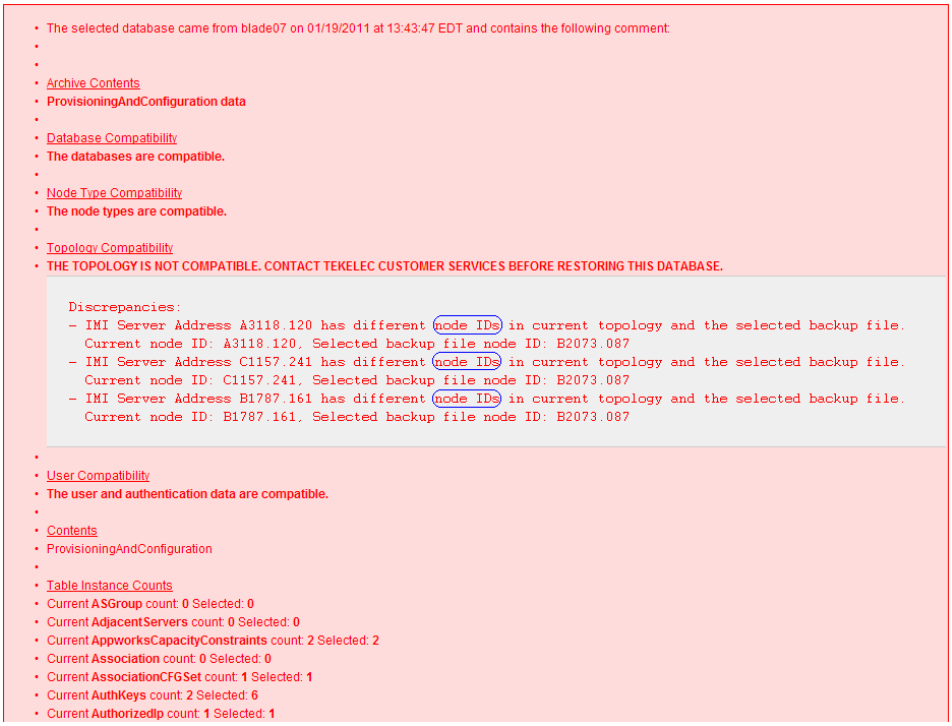
3. A confirmation window will appear, press “OK” to disable Provisioning.


4. The message “Warning Code 002” will appear.</td></tr>
<tr><td>14</td><td>Verify the Archive Contents and Database Compatibility</td><td>
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.


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

Procedure 1. Recovery Scenario 1



- 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.

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

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>**

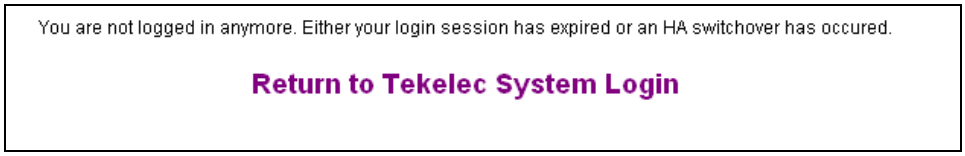
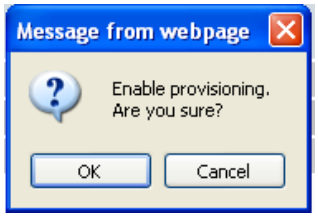
3. Depending on the type of the backup file, restore it using one of the following commands:

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

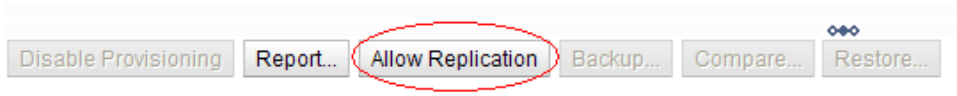
   If the file is a gzip compressed tar file (extension is .tar.gz):
   # **idb.restore -f –z <filename>**

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

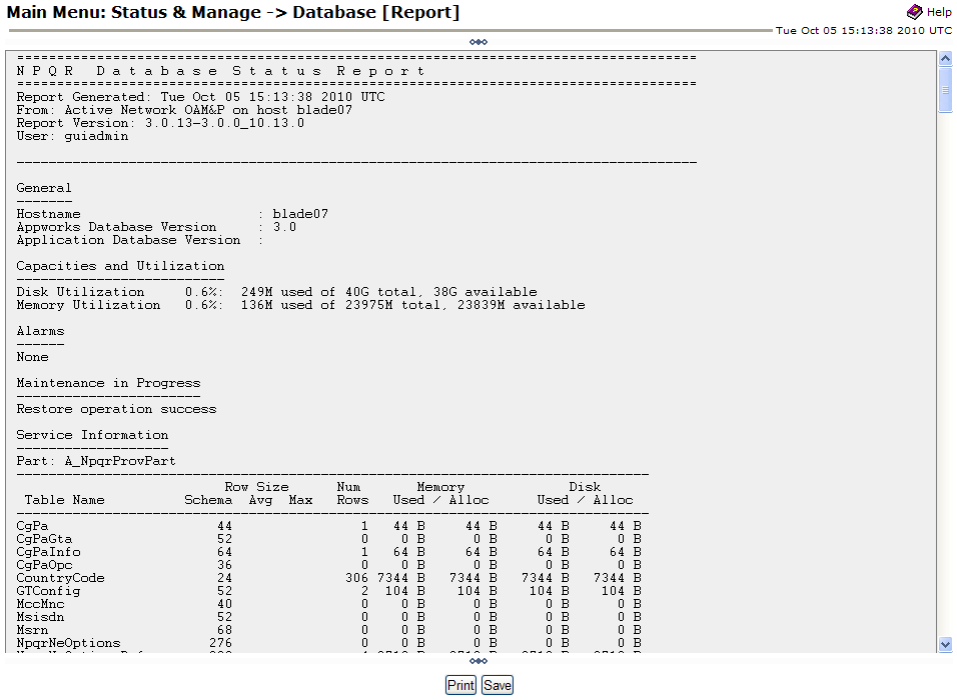
Procedure 1. Recovery Scenario 1

		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  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 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.***
16	Re-enable Provisioning	1. Click on Main Menu->Status & Manage->Database menu item.  2. Click on the "Enable Provisioning" button. A pop-up window will appear to confirm as shown below, press OK. 
17	Recover standby SO server.	Recover the standby SO server: Install the second SO server by executing Reference [5], Procedure "Configure the SOAM Servers, steps 1, 4, 5, 6 and 7 for the second SO Server.

Procedure 1. Recovery Scenario 1

18 ☐	Recover the MP Servers	Execute the following procedures from [5] FOR **EACH** MP that has been recovered: 1."Configure MP Servers", Steps 1, 4, 5, 6 and 7 2. Reapply the signaling Networking Configuration by running the following command from the active NO command line for each MP Server: **/usr/TKLC/appworks/bin/syncApplConfig <MP_Hostame>**
19 ☐	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.
20 ☐	Allow Replication to all Servers	1. Navigate to Status & Manage -> Database 2. If the "Repl Status" is set to "Inhibited", click on the "Allow Replication" button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step.: a. Active NOAMP Server b. Standby NOAMP Server c. Active MP Servers d. Standby MP Servers  Verify that the replication on all servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit" Replication" instead of "Allow Replication".
21 ☐	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**

Procedure 1. Recovery Scenario 1

<table>
<tr><td>22</td><td>Fetch and Store the database Report for the newly restored data and save it</td><td>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:
 

2. Click on “Save” and save the report to your local machine.</td></tr>
<tr><td>23</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.
 
</td></tr>
<tr><td>24</td><td>Verify the Database states</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</td></tr>
<tr><td>25</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 status is as shown below part.</td></tr>
<tr><td>26</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>27</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>28</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>29</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 1. Recovery Scenario 1

30 ☐	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.
31 ☐	Restore GUI Usernames and passwords	If applicable, Execute steps in Section 6 to recover the user and group information restored.
32 ☐	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 Outage with one RMS Server intact)

For a partial outage with an RMS server intact and available; the second RMS is recovered using recovery procedures of base hardware and software. All VMs are recovered using recovery procedures. Database replication 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 Base Hardware and Software for Failed RMS Server.
    - Recover the base hardware. (by replacing the hardware and executing hardware configuration procedures, reference [5]).
    - Recover the Virtual Machines. (by executing procedures from reference [5])
    - Recover the software. (by executing installation procedures, reference [5])
- Recover PM&C if needed
- Recover standby NO Guest
    - Reconfigure the application
- Recover standby SO and MP Guest
    - Reconfigure the Application
- Restart processes and re-enable provisioning and replication.

Procedure 2. Recovery Scenario 2

S T E P #	This procedure performs recovery if 1 RMS server is intact. 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 failed RMS	Recover the failed RMS server by recovering base hardware and software. **Note that if a partial failure occurred that impacts some of the VMs and not the entire server, simply re-IPM the failed VMs using procedure "Install the Software on the VMs" from [5] and skip the rest of this step and step 2.** 1. Gather the documents and required materials listed in Section 3.1. 2. Remove the failed RMS Server and install replacement. 3. Configure and verify the BIOS on the RMS. Execute procedure "Configure the RMS Server BIOS Settings and Update Firmware" from reference [5]. If the Failed RMS hosts the PM&C, execute the following, Otherwise skip to step 2: 4.Execute procedure "Install TVOE 2.0 on First RMS Server" from reference [5]. 5.Execute procedure "First RMS Configuration" from reference [5]. 6.Execute procedure 6 from Appendix Bto recover the PM&C 7.Execute procedure "Load ISOs onto PM&C Server" from reference [5]. 8.Execute procedure "Create NOAMP Guest VMs" on the failed RMS from reference [5]. 9.Execute procedure "Create NOAM Guest VMs" on the failed RMS from reference [5]. 10.Execute procedure "Create MP Guest VMs" on the failed RMS from reference [5]. 11.If applicable, execute procedure "Create IPFE Guest VMs" on the failed RMS from reference [5]. 12. IPM all the guests created in this step using procedure "Install the Software on the VMs" from [5]. Skip to Step 3.
2 ☐	Recover Failed RMS	If the failed RMS does **not** host the PM&C, then execute this step, otherwise skip to the next step: 1.Execute procedure "Install TVOE on Second RMS" from reference [5]. 2.Execute procedure "Configure TVOE on Second RMS Server" from reference [5]. 3.Execute procedure "Create NOAMP Guest VMs" on the failed RMS from reference [5]. 4.Execute procedure "Create NOAM Guest VMs" on the failed RMS from reference [5]. 5.Execute procedure "Create MP Guest VMs" on the failed RMS from reference [5]. 6.If applicable, execute procedure "Create IPFE Guest VMs" on the failed RMS from reference [5]. 7. IPM all the guests created in this step using procedure "Install the Software on the VMs" from [5].

Procedure 2. Recovery Scenario 2

<table>
<tr><td>3</td><td>Recover the application</td><td>Recover the application by executing the following steps:

Note that if a partial failure occurred that impacts some of the VMs and not the entire server, execute the steps that relate to the failed VM.

1. Install the application on all VMs of the failed RMS using procedure “Install the Software on the VMs” from [5].

<u>NO:</u>
2. Configure the newly installed NO by executing procedure “Configure the Second NOAMP Server, from [5] steps 1, 2, 4, 5 and 6.
3. 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”.
4. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered server and Clicking on “Restart”.

<u>SO:</u>
5. From the NO VIP GUI, set the server HA state of the newly recovered SO 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.
6. 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”.
7. Configure the newly installed application by executing procedure “Configure the SOAM Server, from [5] steps 1, 2, 4, 5 and 6.
8. 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”.
9. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered server and Clicking on “Restart”.

<u>MP/IPFE:</u>
10. 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”.
11. Execute the following procedures from [5] ”Configure MP Servers”, Steps 1, 2, 4, 5 and 6
12. 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”.
13. Reapply the signaling Networking Configuration by running the following command from the active NO command line:
/usr/TKLC/appworks/bin/syncApplConfig <Recovered_MP_Hostame>

14. Restart the application by Navigating to Main Menu->Status & Manage->Server, then selecting the recovered servers and Clicking on “Restart”.</td></tr>
<tr><td>4</td><td>Remove Forced Standby</td><td>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</td></tr>
<tr><td>5</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>
</table>

Procedure 2. Recovery Scenario 2

<table>
<tr><td>6</td><td>Verify the Database state of the newly restored server</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>7</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>8</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>9</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>10</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>11</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>12</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>
<tr><td>13</td><td>Examine All Alarms</td><td>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</td></tr>
<tr><td>14</td><td>Backup and archive all the databases from the recovered system</td><td>Execute Appendix A back up the Configuration databases:

Disaster Recovery Procedure is Complete</td></tr>
</table>

End of Procedure

6 RESOLVING USER CREDENTIAL ISSUES AFTER DATABASE RESTORE

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

6.1 Restoring a Deleted User

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

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

6.1.1 To Keep the Restored User

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

Before restoration,

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

After restoration

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

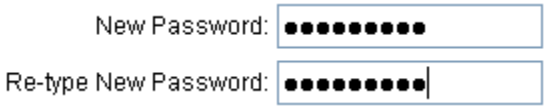
1. Navagate to the user administration screen.

   Main Menu: Administration->'User'

2. Select the user.

3. Click the Change Password button.

4. Enter a new password.

5. Click the Continue button.

6.1.2 To Remove the Restored User

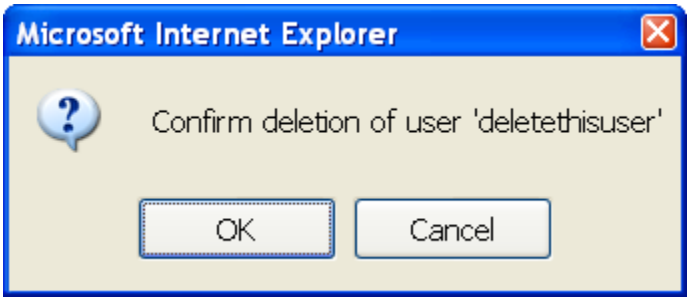
Perform this step to remove users that will be restored by system restoration.

After restoration, delete all users in this category.

1. Navagate to the user administration screen.

   Main Menu: Administration->'User'

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



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,

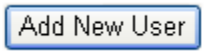
- Verify that you have access to a user with administrator permissions that is not affected.
- Contact each user that is affected and notify them that you will reset their password during this maintenance operation.
- Log in and record the username, group, timezone, comment, and enabled values for each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

After restoration

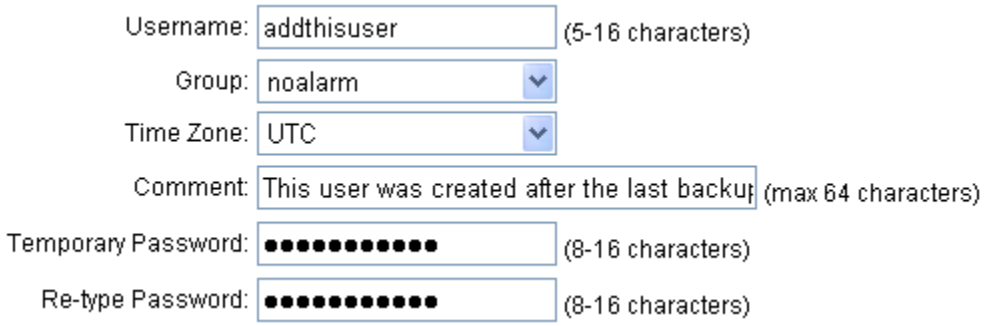
- Log in and re-create each of the affected users using the information recorded above

1. Navagate to the user administration screen.

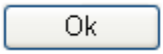
2. Click the Add New User button.



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



4. Click the OK button.



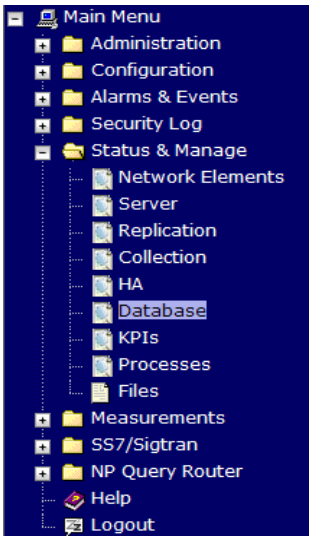
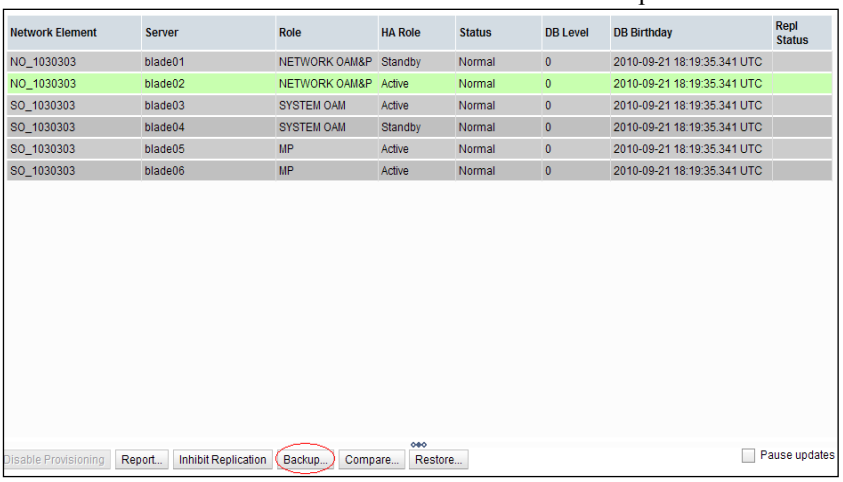
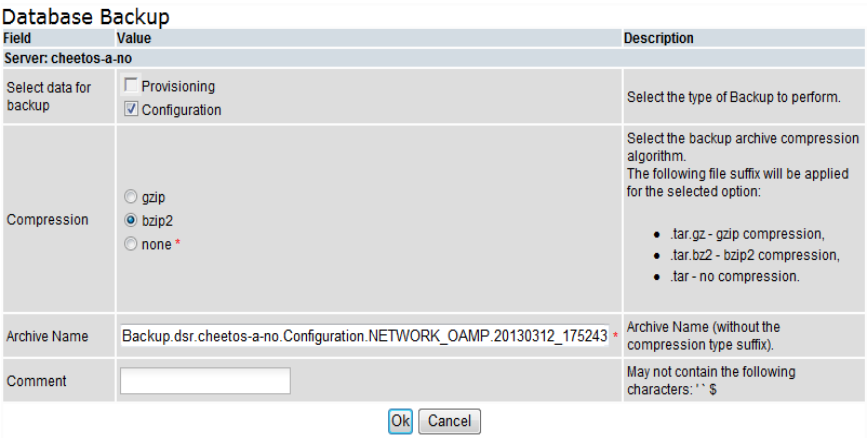
- Reset the passwords for all users in this category. See the steps in section 6.1.1 for resetting passwords for a user.

Appendix A. EAGLEXG DSR 4.1 Database Backup

Procedure 3: DSR 4.1 Database Backup

S T E P #		
	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 4.1 "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.	
1.	**Login into NO (or SO) XMI VIP IP Address**	Login using the "guiadmin" credentials.

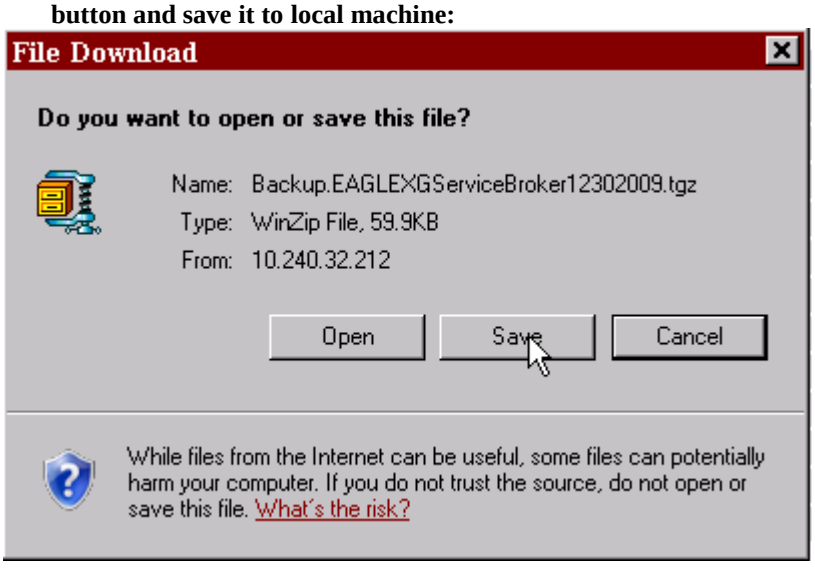
Procedure 3: DSR 4.1 Database Backup

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 :  3. Make sure that the checkboxes next to Configuration is checked. Then enter a filename for the backup and press "OK". 4. 

Procedure 3: DSR 4.1 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 | 4. Verify the existence of the backed up configuration back up file as shown above.
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 | **2. File download dialog box will be displayed as shown, click on the save button and save it to local machine:**

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



Procedure 3: DSR 4.1 Database Backup

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 Eagle XG DSR 4.1 complete.

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

Procedure 4: 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 [6] *PM&C Disaster Recover* on instructions how to recover a PM&C Server.

Procedure 5: 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 Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	

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

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

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 VIP address of the DR DSR as root and make it primary	1. Login via SSH to VIP of 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

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 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 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	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