Oracle® Diameter Signaling Router
DSR 4.X/5.X 3-tier Disaster Recovery Guide
Release 5.0
909-2246-001

December 2013
Disaster Recovery Guide

Copyright © 2012, 2013 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Phone: 1-888-367-8552 or 919-460-2150 (international)
FAX: 919-460-2126
TABLE OF CONTENTS

1 INTRODUCTION .............................................................................................................. 5
  1.1 Purpose and Scope ..................................................................................................... 5
  1.2 References .................................................................................................................. 5
  1.3 Software Release Numbering .................................................................................... 5
  1.4 Acronyms .................................................................................................................... 6
  1.5 Terminology ................................................................................................................ 6

2 GENERAL DESCRIPTION ................................................................................................. 7
  2.1 Complete Server Outage (All servers) ......................................................................... 7
  2.2 Partial Server Outage with one NO Server intact and both SOs failed ....................... 7
  2.3 Partial Server Outage with both NO Servers failed and one SO server Intact .......... 7
  2.4 Partial Server Outage with one NO and one SO Server Intact ..................................... 7

3 PROCEDURE OVERVIEW ................................................................................................. 8
  3.1 Required Materials ..................................................................................................... 8
  3.2 Disaster Recovery Strategy ......................................................................................... 9

4 PROCEDURE PREPARATION ............................................................................................ 10

5 DISASTER RECOVERY PROCEDURE ............................................................................ 11
  5.1 Recovering and Restoring System Configuration ....................................................... 12
    5.1.1 Recovery Scenario 1 (Complete Server Outage) .................................................. 12
    5.1.2 Recovery Scenario 2 (Partial Server Outage with one NO Server intact and both SOs
        failed) 26
    5.1.3 Recovery Scenario 3 (Partial Server Outage with both NO Servers failed and one SO
        Server intact) ........................................................................................................ 35
    5.1.4 Recovery Scenario 4 (Partial Server Outage with one NO Server and one SO Server
        Intact) 46
    5.1.5 Recovery Scenario 5 (Both NO Servers failed with DR NO available) .................. 52

6 RESOLVING USER CREDENTIAL ISSUES AFTER DATABASE RESTORE ................... 54
  6.1 Restoring a Deleted User ............................................................................................. 54
    6.1.1 To Keep the Restored User .................................................................................... 54
    6.1.2 To Remove the Restored User ............................................................................... 54
  6.2 Restoring a Modified User .......................................................................................... 55
  6.3 Restoring an Archive that Does not Contain a Current User ....................................... 55

Appendix A. EAGLEXG DSR 4.x/5.x Database Backup ...................................................... 57
Appendix B. Recovering/Replacing a Failed 3rd party components (Switches, OAs) ......... 61
Appendix C. Switching a DR Site to Primary ................................................................. 64
Recovery Steps .................................................................................................................. 64

Appendix D. Returning a Recovered Site to Primary ..................................................... 67
Recovery Steps .................................................................................................................. 67

Appendix E. Workarounds for Issues/PR not fixed in this release.................................. 69

Appendix F. Contacting Tekelec .................................................................................... 70

List of Figures
Figure 1: Determining Recovery Scenario...................................................................... 9

List of Tables
Table 2. Terminology ..................................................................................................... 6
Table 3. Recovery Scenarios .......................................................................................... 10

List of Procedures
Procedure 1. Recovery Scenario 1 .................................................................................. 13
Procedure 2. Recovery Scenario 2 .................................................................................. 27
Procedure 3. Recovery Scenario 3 .................................................................................. 36
Procedure 4. Recovery Scenario 4 .................................................................................. 47
Procedure 5. Recovery Scenario 5 .................................................................................. 53
Procedure 5: DSR 4.x/5.x Database Backup................................................................... 57
Procedure 6: Recovering a failed Aggregation PM&C Server ....................................... 61
Procedure 7: Recovering a failed Aggregation Switch (Cisco 4948E / 4948E-F)................ 61
Procedure 8: Recovering a failed Enclosure Switch (Cisco 3020) ................................. 62
Procedure 9: Recovering a failed Enclosure Switch (HP 6120XG) ................................. 62
Procedure 9: Recovering a failed Enclosure Switch (HP 6125XG) ................................. 63
Procedure 10: Recovering a failed Enclosure OA........................................................... 63
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)
[3] TPD Initial Product Manufacture, 909-2130-001
[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
[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
[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

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

1.5 Terminology

Table 1. Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base hardware</td>
<td>Base hardware includes all hardware components (bare metal) and electrical wiring to allow a server to power on.</td>
</tr>
<tr>
<td>Base software</td>
<td>Base software includes installing the server’s operating system: Tekelec Platform Distribution (TPD).</td>
</tr>
<tr>
<td>Failed server</td>
<td>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.</td>
</tr>
</tbody>
</table>
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
     o Both NO servers failed
     o All SO servers failed
   Recovery of one or more servers with at least one Network OAM&P server intact
     o 1 or both NO servers intact
     o 1 or more SO or MP servers failed
   Recovery of the Network OAM&P pair with one or more System OAM servers intact
     o Both NO servers failed
     o 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
     o 1 or both NO servers intact
     o 1 or more SO servers intact
     o 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.
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.
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 Diagram](image-url)
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

<table>
<thead>
<tr>
<th>Recovery Scenario</th>
<th>Failure Conditions</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• Both NO servers failed.</td>
<td>Execute Section 5.1.1, Procedure 1.</td>
</tr>
<tr>
<td></td>
<td>• All SO servers failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>• At least 1 NO server is intact and available.</td>
<td>Execute Section 5.1.2, Procedure 2.</td>
</tr>
<tr>
<td></td>
<td>• All SO servers failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>• Both NO servers failed.</td>
<td>Execute Section 5.1.3, Procedure 3.</td>
</tr>
<tr>
<td></td>
<td>• At least 1 SO server is intact and available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>• At least 1 NO server is intact and available.</td>
<td>Execute Section 5.1.4, Procedure 4.</td>
</tr>
<tr>
<td></td>
<td>• At least 1 SO server is intact and available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 or more MP servers have failed.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>• Both NO servers failed.</td>
<td>Execute Section 5.1.4, Procedure 5.</td>
</tr>
<tr>
<td></td>
<td>• DR NO is Available</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SO servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MP servers may or may not be failed.</td>
<td></td>
</tr>
</tbody>
</table>
5 DISASTER RECOVERY PROCEDURE

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

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

**** WARNING *****

**** WARNING *****

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

Recovering Base Hardware

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | 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.  
  5. Load any firmware upgrades using [1].  
  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.  |
| 2    | Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.  
  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 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)  
| 4    | 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click on Main Menu-&gt;Status &amp; Manage-&gt;Database</td>
</tr>
<tr>
<td>2</td>
<td>Disable Provisioning</td>
</tr>
<tr>
<td>3</td>
<td>Click on “Browse” and Locate the backup file and click on “Open” as shown below.</td>
</tr>
<tr>
<td>4</td>
<td>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.</td>
</tr>
</tbody>
</table>
2. Disable Provisioning by clicking on “Disable Provisioning” button at the bottom of the screen as shown below.

![Disable Provisioning](image)

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

![Confirmation Window](image)


7. Verify the Archive Contents and Database Compatibility

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

![Compare Screen](image)

2. The following screen is displayed; click the radio button for the restored database file that
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 TEGICLIC CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.

   Discrepancies:
   - IBM Server Address A310A120 has different node ID in current topology and the selected backup file.
     Current node ID: A310A120. Selected backup file node ID: B3797.161.
   - IBM Server Address C357C441 has different node ID in current topology and the selected backup file.
     Current node ID: C357C441. Selected backup file node ID: B3797.161.
   - IBM Server address B3797.161 has different node ID in current topology and the selected backup file.

- User Compatibility:
  The user and authentication data are compatible.

- Contents:
  ProvisioningAndConfiguration data

- Table Instance Counts:
  - Current AGroup count 0 Selected 0
  - Current AdjacentServers count 0 Selected 0
  - Current AccessRequests/Capacities/Constraints count 2 Selected 2
  - Current Association count 0 Selected 0
  - Current Association/ISetoSet count 1 Selected 1
  - Current AuthKeys count 2 Selected 2
  - Current Authorization/IDtoSet 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click on Main Menu-&gt;Status &amp; Manage-&gt;Database</td>
</tr>
<tr>
<td>2.</td>
<td>Select the Active NO Server, and click on “Restore” as shown below.</td>
</tr>
<tr>
<td>3.</td>
<td>The following screen will be displayed. Select the proper back up provisioning and configuration file.</td>
</tr>
</tbody>
</table>

**Database Restore**

- Select archive to Restore on server: blade02
- 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
- Node IDs: 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
- Node ID: 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
- Node ID: A3118.161 has different node IDs in current topology and the selected backup file.
- Current node ID: A3118.161. Selected backup file node ID: B2073.087

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:

   ![Logout Screen]

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

   Return to Tekelec System Login

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

<table>
<thead>
<tr>
<th></th>
<th>Re-enable Provisioning</th>
<th>Recover standby NO server</th>
<th>Recover active SO server</th>
<th>Upload the backed up SO database file from Remote location into File Management Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>1. Click on Main Menu-&gt;Status &amp; Manage-&gt;Database menu item. Enable Provisioning</td>
<td>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].</td>
<td>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.</td>
<td>1. Browse to Main Menu-&gt;Status &amp; Manage-&gt;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.</td>
</tr>
</tbody>
</table>
**Procedure 1. Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click on Main Menu-&gt;Status &amp; Manage-&gt;Database</td>
</tr>
<tr>
<td>2.</td>
<td>Disable Provisioning by clicking on “Disable Provisioning” button at the bottom of the screen as shown below.</td>
</tr>
<tr>
<td>3.</td>
<td>A confirmation window will appear, press “OK” to disable Provisioning.</td>
</tr>
</tbody>
</table>

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.
Procedure 1. Recovery Scenario 1

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](image)

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 blade02 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 TERELEC CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.

     Discrepancies:
     - DK Server Address A3108 120 has different node ID in current topology and the selected backup file. Current node ID: A3108 120, Selected backup file node ID: B2073 387
     - DK Server Address C1157 241 has different node ID in current topology and the selected backup file. Current node ID: C1157 241, Selected backup file node ID: B2073 387
     - DK Server Address B3787 141 has different node ID in current topology and the selected backup file. Current node ID: B3787 141, Selected backup file node ID: B2073 387

     - User Compatibility
       - The user and authentication data are compatible.
     - Contexts
       - ProvisioningAndConfiguration
     - Table Instance Counts
       - Current A Group count 0 Selected 0
       - Current AdjacentServers count 0 Selected 0
       - Current AppearanceCapacityConstraints count 2 Selected 2
       - Current Association count 0 Selected 0
       - Current AssociationUser count 1 Selected 1
       - Current AuthKeys count 2 Selected 2
       - Current AuthorityType 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
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>SSH to the SO terminal as <code>root</code></td>
</tr>
<tr>
<td>2.</td>
<td>Verify that the SO database backup file that was uploaded in step 12 is located under <code>/var/TKLC/db/filemgmt</code> by running the following command: &lt;br&gt;<code># ls /var/TKLC/db/filemgmt/&lt;filename&gt;</code></td>
</tr>
<tr>
<td>3.</td>
<td>Depending on the type of the backup file, restore it using one of the following commands: &lt;br&gt;If the file is a bzip2 compressed tar file (extension is <code>.tar.bz2</code>): &lt;br&gt;<code># idb.restore -f -j &lt;filename&gt;</code> &lt;br&gt;If the file is a gzip compressed tar file (extension is <code>.tar.gz</code>): &lt;br&gt;<code># idb.restore -f -z &lt;filename&gt;</code> &lt;br&gt;If the file is an uncompressed tar file (extension is <code>.tar</code>): &lt;br&gt;<code># idb.restore -f -n &lt;filename&gt;</code></td>
</tr>
<tr>
<td>4.</td>
<td>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: &lt;br&gt;<code>...&lt;br&gt;- Reinitialize MySQL&lt;br&gt;- Unlocking idbsvc for each part&lt;br&gt;- Sync Parts to disk</code></td>
</tr>
<tr>
<td>5.</td>
<td><strong>NOTE:</strong> 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 &lt;br&gt;<strong>You are not logged in anymore. Either your login session has expired or an HA switchover has occurred.</strong> &lt;br&gt;&lt;br&gt;<strong>Return to Tekelec System Login</strong></td>
</tr>
<tr>
<td>6.</td>
<td>Log in Back into GUI VIP by clicking “Continue to this Website”</td>
</tr>
<tr>
<td>7.</td>
<td>Login using the guiadmin login and password into the GUI</td>
</tr>
<tr>
<td>8.</td>
<td>Wait for 5-10 minutes for the System to stabilize with the new topology.</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Re-enable Provisioning</td>
</tr>
<tr>
<td>1.</td>
<td>Log into the Active NO GUI</td>
</tr>
</tbody>
</table>
| 2.   | Click on Main Menu->Status & Manage->Database menu item.  
|      | ![Enable Provisioning](image)
| 3.   | Click on the “Enable Provisioning” button. A pop-up window will appear to confirm as shown below, press OK. |
| 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:  
| 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

#### 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”.

#### 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

#### 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:

   ![Database Report](image)

2. Click on “Save” and save the report to your local machine.
**Procedure 1. Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td><strong>DSR 4.X Recovery ONLY: Optimize Comcol memory usage on NO and SO</strong></td>
</tr>
</tbody>
</table>
|      | 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. |
| 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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

**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.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Recover standby NO server (if needed). | 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.  
7. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details.  
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]  
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”.

---

909-2246-001  27 of 70
### 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.
4. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details.
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.
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.

#### 4. Disable Provisioning

1. From the NO GUI, Click on Main Menu->Status & Manage->Database
### Procedure 2. Recovery Scenario 2

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

- Select “Disable Provisioning” from the menu.

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

![Message from webpage](image)

- Click “OK” to confirm.


- Verify that the output window matches the screen below.

#### 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](image)

3. Verify that the output window matches the screen below.
Disaster Recovery Guide

Procedure 2. Recovery Scenario 2

Database Restore Confirm

The selected database came from FZTEST-N01 on 10/22/2013 at 02:15:02 EDT and contains the following contents:

- 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. 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:

   # Is /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.

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 occurred.

   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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Re-enable Provisioning</td>
</tr>
<tr>
<td></td>
<td>1. Click on Main Menu-&gt;Status &amp; Manage-&gt;Database menu item.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Enable Provisioning" /></td>
</tr>
<tr>
<td></td>
<td>2. Click on the “Enable Provisioning” button. A pop-up window will appear to confirm as shown below, press OK.</td>
</tr>
<tr>
<td>8</td>
<td>Recover remaining SO servers.</td>
</tr>
<tr>
<td></td>
<td>Recover the remaining SO servers (standby, spare) by repeating the following step for each SO Server:</td>
</tr>
<tr>
<td></td>
<td>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’.</td>
</tr>
<tr>
<td>9</td>
<td>Recover the MP Servers (also applies to IPFE servers)</td>
</tr>
<tr>
<td></td>
<td>Execute the following procedures from [5] (4.X) or [7] (5.X) FOR EACH MP that has been recovered:</td>
</tr>
<tr>
<td></td>
<td>1. &quot;Configure MP Blades Servers&quot;, Steps 1, 4, 5, 6 and 7</td>
</tr>
<tr>
<td></td>
<td>2. <strong>(DSR 4.X ONLY):</strong> Reapply the signaling Networking Configuration by running the following command from the active NO command line for each MP Server:</td>
</tr>
<tr>
<td></td>
<td><code>/usr/TKLC/appworks/bin/syncApplConfig &lt;MP_Hostame&gt;</code></td>
</tr>
<tr>
<td></td>
<td>3. If IPFE servers are being recovered, execute Procedure 5 of [20] for any applicable IPFE servers.</td>
</tr>
<tr>
<td>10</td>
<td>DSR 5.X Recovery Only: Re-Sync NTP if Necessary (Optional)</td>
</tr>
<tr>
<td></td>
<td>Navigate to Status &amp; Manage -&gt; Server, then select each server that has been recovered and click NTP Sync.</td>
</tr>
<tr>
<td>11</td>
<td>Restart Application Processes</td>
</tr>
<tr>
<td></td>
<td>Restart the Application by Navigating to Status &amp; Manage -&gt; Server, then select each server that has been recovered and clicking on Restart at the bottom of the screen.</td>
</tr>
</tbody>
</table>

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

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

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)

*NOTE: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.*
Procedure 2. Recovery Scenario 2

12 Allow Replication to all Servers

1. Navigate to Status & Manage -> Database
2. If the "Rep 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:
   - Active NOAMP Server
   - Standby NOAMP Server
   - Active SOAM Server
   - Standby SOAM Server
   - Spare SOAM Server (if applicable)
   - Active DR NOAM Server
   - 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:

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".

2. Click on "Save" and save the report to your local machine.
## Procedure 2. Recovery Scenario 2

### Step 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.

### Step 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
  ```

### Step 17. Verify Replication between servers.

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

<table>
<thead>
<tr>
<th>blade02</th>
<th>Replicating</th>
<th>To</th>
<th>blade01</th>
<th>Active</th>
<th>0</th>
</tr>
</thead>
</table>

### Step 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”.

### Step 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.

### Step 20. Verify the local node info

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

### Step 21. Verify the peer node info

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

### Step 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

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 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 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

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.**
   - **Note:** If necessary, Refer to [8] *PM&C Disaster Recovery* 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.
   6. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details.
   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]
   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”.

---

**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.
Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Obtain the most recent database backup file from external backup sources (e.g., file servers, Netbackup) or tape backup sources. Determine network configuration data.</td>
</tr>
<tr>
<td></td>
<td>1. Using procedures within your organization's process (e.g., 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, coordinate with the customer's Netbackup administrator to obtain the proper backup files.</td>
</tr>
<tr>
<td></td>
<td>2. From required materials list in Section 3.1; use site survey documents and Network Element report (if available), to determine network configuration data.</td>
</tr>
<tr>
<td>3.</td>
<td>Execute procedures from EAGLEXG DSR 4.x/5.x Installation User's Guide.</td>
</tr>
<tr>
<td></td>
<td>1. Verify the networking data for Network Elements. Use the backup copy of network configuration data and site surveys (from Step 2).</td>
</tr>
<tr>
<td>4.</td>
<td>Login into the NO XMI Address</td>
</tr>
<tr>
<td>5.</td>
<td>Upload the backed up database file from Remote location into File Management Area.</td>
</tr>
<tr>
<td></td>
<td>1. Log into the first NO GUI.</td>
</tr>
<tr>
<td></td>
<td>2. Browse to Main Menu-&gt;Status &amp; Manage-&gt;Files</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><img src="" alt="Screen Shot" /></td>
</tr>
<tr>
<td></td>
<td>4. Click on “Browse” and Locate the backup file and click on “Open” as shown below.</td>
</tr>
<tr>
<td></td>
<td><img src="" alt="Screen Shot" /></td>
</tr>
</tbody>
</table>
Procedure 3. Recovery Scenario 3

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

   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.

1. Select the Active NO Server and click on the "Compare".

<table>
<thead>
<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>
</thead>
<tbody>
<tr>
<td>NO_200060101</td>
<td>HPC1sl001</td>
<td>NETWORK OAM&amp;P</td>
<td>Active</td>
<td>Normal</td>
<td>0</td>
<td>2011-02-16 19:44:17.842 UTC</td>
</tr>
<tr>
<td>NO_200060101</td>
<td>HPC1sl002</td>
<td>NETWORK OAM&amp;P</td>
<td>Standby</td>
<td>Normal</td>
<td>0</td>
<td>2011-02-16 19:44:17.842 UTC</td>
</tr>
<tr>
<td>NO_200060101</td>
<td>HPC1sl003</td>
<td>NP</td>
<td>Active</td>
<td>Normal</td>
<td>0</td>
<td>2011-02-16 19:44:17.842 UTC</td>
</tr>
<tr>
<td>NO_200060101</td>
<td>HPC1sl004</td>
<td>NP</td>
<td>Standby</td>
<td>Normal</td>
<td>0</td>
<td>2011-02-16 19:44:17.842 UTC</td>
</tr>
</tbody>
</table>

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.

The database compare screen shows the options to compare the archived databases with the current database. The archive files are listed on the left side, and the current database file is selected on the right side.

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

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 database 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.

Restore the Database

1. Click on Main Menu->Status & Manage->Database
2. Select the Active NO Server, and click on “Restore” as shown below.
Procedure 3. Recovery Scenario 3

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

Database Restore

Select archive to restore on server: bladed02

Archive
- Backup node bladed02, Configuration NETWORK_DAIMP 20100808_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20100908_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20100908_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20101001_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20100908_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20101001_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20100908_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20100908_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20101001_021502 AUTO.tar
- Backup node bladed02, Configuration NETWORK_DAIMP 20100908_021502 AUTO.tar

Select the archive to restore on bladed02.

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.

Incompatible database selected

- JM Server Address A3118.120 has different node ID in current topology and the selected backup file.
- JM Server Address A3118.120 has different node ID in current topology and the selected backup file.
- JM Server Address C2234.141 has different node ID in current topology and the selected backup file.
- JM Server Address C3473.24.1 has different node ID in current topology and the selected backup file.
- JM Server Address 5073.611 has different node ID in current topology and the selected backup file.
- JM Server Address 5073.611 has different node ID in current topology and the selected backup file.

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

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.**

Re-enable Provisioning

1. Click on Main Menu->Status & Manage->Database menu item.

   ![Enable Provisioning](image)

   2. Click on the “Enable Provisioning” button. A pop-up window will appear to confirm as shown below, press OK.
## Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 10   | Restore `/etc/hosts` file of active NO server. Release 5.X: From the recovered NO server command line, execute:  
   # `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 |

---

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]
```

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Command/Details</th>
</tr>
</thead>
</table>
| 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. |
| 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 is 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Recover standby NO server (if needed).</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Recover the standby NO server (if needed) by recovering base hardware and software.</td>
</tr>
</tbody>
</table>

**Note:** If necessary, refer to [8] *PM&C Disaster Recovery* 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. 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.
6. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details.
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]
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 Standby” 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.

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.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Recover SO servers (if needed).</td>
</tr>
<tr>
<td></td>
<td>Recover the SO server(s) (if needed) by recovering base hardware and software.</td>
</tr>
<tr>
<td></td>
<td>If both SO servers are intact and available, skip this step and go to Step 3.</td>
</tr>
<tr>
<td></td>
<td>Execute the following for any SO server that has failed:</td>
</tr>
<tr>
<td></td>
<td>1. Gather the documents and required materials listed in Section 3.1.</td>
</tr>
<tr>
<td></td>
<td>2. From the NO VIP GUI, set the server HA state to “Forced Standby” by navigating to Main Menu-&gt;HA, then clicking on Edit and setting the “Max Allowed HA Role” to Standby for the SO in question and pressing OK.</td>
</tr>
<tr>
<td></td>
<td>3. From the NO VIP GUI, Inhibit replication to the standby SO by navigating to Main Menu-&gt;Status &amp; Manage-&gt;Database, then selecting the SO in question and clicking on “Inhibit Replication”.</td>
</tr>
<tr>
<td></td>
<td>4. Remove the failed HP c-Class Blade and install the replacement into the enclosure.</td>
</tr>
<tr>
<td></td>
<td>7. Upgrade the blade firmware and load an errata updates if needed. Refer to [1] for more details.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>13. Install the application on the SO using procedure “Install the Application Software on the Blades” from [5].</td>
</tr>
<tr>
<td></td>
<td>15. Re-enable Replication to the restored SO by navigating to Main Menu-&gt;Status &amp; Manage-&gt;Database, then selecting the SO in question and clicking on “Allow Replication”.</td>
</tr>
<tr>
<td></td>
<td>16. Restart the application by Navigating to Main Menu-&gt;Status &amp; Manage-&gt;Server, then selecting the recovered server and Clicking on “Restart”.</td>
</tr>
</tbody>
</table>
|      | 17. 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 Active for the SO in question and pressing OK.
Procedure 4. Recovery Scenario

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Recover MP servers (if needed).</td>
</tr>
</tbody>
</table>

  - 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)
    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.
    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 -> 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.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Remove Forced Standby</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Optimize Comcol memory usage on recovered NO and SO</td>
</tr>
</tbody>
</table>

  - 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>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 6    | **Optimize Comcol memory usage on DA-MP** *(Execute for 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 |  |
| 7    | **Verify Replication between servers.**  
1. Click on Main Menu->Status and Manager->Replication  
2. Verify that replication is occurring between servers.  
| | ![Replication Status](image) |
| 8    | **Verify the Database state of the newly restored blade**  
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 |  |
|   | ![Database Status](image) |
| 9    | **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 status is either Active or Standby as shown below |  |
|   | ![HA Status](image) |
| 10   | **Verify the local node info**  
1. Click on Main Menu->Diameter->Configuration->Local Node  
2. Verify that all the local nodes are listed. |  |
| 11   | **Re-install NetBackup (Optional)**  
1. If NetBackup was previously installed on the system, follow the procedure in [5], Appendix K to reinstall it. |  |
| 12   | **Verify the peer node info**  
1. Click on Main Menu->Diameter->Configuration->Peer Node  
2. Verify that all the peer nodes are listed. |  |
| 13   | **Verify the Connections info**  
1. Click on Main Menu->Diameter->Configuration->Connections  
2. Verify that all the peer nodes are listed. |  |
| 14   | **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. |  |
Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 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 is 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

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.

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. Navigate 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. Navigate 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.

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.
Disaster Recovery Guide

- 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. Navigate to the user administration screen.

   **Main Menu: Administration->'User'**

2. Click the Add New User button.

   ![Add New User button](image)

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

   - **Username:** addthisuser (5-16 characters)
   - **Group:** noalarm
   - **Time Zone:** UTC
   - **Comment:** This user was created after the last backup (max 64 characters)
   - **Temporary Password:** ●●●●●●●●●● (8-16 characters)
   - **Re-type Password:** ●●●●●●●●●● (8-16 characters)

4. Click the OK button.

   ![Click button](image)

- Reset the passwords for all users in this category. See the steps in section 6.1.1 for resetting passwords for a user.
Procedure 6: DSR 4.x/5.x Database Backup

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.

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Login into NO (or SO) XMI VIP IP Address</td>
</tr>
</tbody>
</table>

Login using the “guiadmin” credentials.
Procedure 6: DSR 4.x/5.x Database Backup

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”.

Backup Configuration data for the system.
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'
```

<table>
<thead>
<tr>
<th>Action</th>
<th>File Name</th>
<th>Size</th>
<th>Timestamp</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>872-1734.42.0.8.20.33.0.0.006.60</td>
<td>473.4 MB</td>
<td>2009-Dec-09 11:22:00 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>872-1734.42.0.8.20.33.0.31.0.0.006.60</td>
<td>689.1 MB</td>
<td>2009-Dec-24 05:42:14 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Applications</td>
<td>4.2 MB</td>
<td>2009-Dec-03 03:53:05 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Backup EAI Services Broker12010109.dmp</td>
<td>80.9 MB</td>
<td>2009-Dec-30 23:19:46 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Events_20091206_115716.csv</td>
<td>1.1 KB</td>
<td>2009-Dec-08 11:57:17 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Events_20091205_175405.csv</td>
<td>6.2 KB</td>
<td>2009-Dec-24 13:34:00 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Events_20091207_155105.csv</td>
<td>5.8 KB</td>
<td>2009-Dec-26 05:21:08 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>TKLConfigData.sql</td>
<td>1.4 KB</td>
<td>2009-Dec-03 15:25:56 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Upgrade Backup TKLDB2 2.0.3_20091128-01-07184</td>
<td>389.3 KB</td>
<td>2009-Dec-06 12:37:56 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Upgrade Backup TKLDB2 2.0.3_20100126-01-07184</td>
<td>407.9 KB</td>
<td>2009-Dec-24 06:39:18 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>upgrade.log</td>
<td>2.6 KB</td>
<td>2009-Dec-24 06:47:36 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>upgrade.log</td>
<td>78.3 KB</td>
<td>2009-Dec-24 06:47:36 UTC</td>
<td>Delete</td>
</tr>
</tbody>
</table>

4. Verify the existence of the backed up configuration back up file as shown above.
Disaster Recovery Guide

DSR 4.x/5.x 3-tier Disaster Recovery

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

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Filename</th>
<th>Size (MB)</th>
<th>Time/Stamp</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>AppNet.xml</td>
<td>4.2 MB</td>
<td>2008-Dec-03 14:53:05 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Backup_EAGLEXGServiceBroker12302008.tgz</td>
<td>19.3 MB</td>
<td>2009-Dec-19 12:57:04 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Events_0001229_152163.dat</td>
<td>6 MB</td>
<td>2009-Dec-28 15:21:00 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>Events_0001229_152163.dat</td>
<td>5 MB</td>
<td>2009-Dec-28 15:21:00 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>THLCConfigData.sh</td>
<td>1.4 MB</td>
<td>2009-Dec-09 15:25:50 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>UpgradeBackup_TDS3CM1-20.0-20.30.8.68651216.071794</td>
<td>309.3 MB</td>
<td>2009-Dec-19 12:57:04 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>UpgradeBackup_TDS3CM1-20.0-20.30.8.68651224.0713917</td>
<td>407.7 MB</td>
<td>2009-Dec-24 06:26:10 UTC</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete</td>
<td>upgrade.dat</td>
<td>2.6 MB</td>
<td>2009-Dec-24 06:47:39 UTC</td>
<td>Delete</td>
</tr>
</tbody>
</table>

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

![File Download](image)

3. **Upload the image to secure location for future disaster recovery of entire system.**

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

5. **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**

<table>
<thead>
<tr>
<th>STEP</th>
<th>The intent of this procedure is to recover a failed PM&amp;C Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.</td>
</tr>
<tr>
<td>1.</td>
<td>Refer to [8] PM&amp;C Disaster Recovery on instructions how to recover a PM&amp;C Server.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>STEP</th>
<th>The intent of this procedure is to recover a failed Aggregation (4948E / 4948E-F) Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prerequisites for this procedure are:</td>
</tr>
<tr>
<td></td>
<td>• A copy of the networking xml configuration files</td>
</tr>
<tr>
<td></td>
<td>• A copy of HP Misc Firmware DVD or ISO</td>
</tr>
<tr>
<td></td>
<td>• IP address and hostname of the failed switch</td>
</tr>
<tr>
<td></td>
<td>• Rack Mount position of the failed switch</td>
</tr>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.</td>
</tr>
</tbody>
</table>
| 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)

| STEP # | 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.

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.

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

| STEP # | 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.
### Procedure 10: Recovering a failed Enclosure Switch (HP 6120XG)

1. Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:
   
   ```bash
   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)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The intent of this procedure is to recover a failed Enclosure (6125XG) Switch.</td>
</tr>
<tr>
<td></td>
<td>Prerequisites for this procedure are:</td>
</tr>
<tr>
<td></td>
<td>• A copy of the networking xml configuration files</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.</td>
</tr>
</tbody>
</table>

1. Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:

   ```bash
   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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The intent of this procedure is to recover a failed Enclosure Onboard Administrator Switch.</td>
</tr>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.</td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th></th>
<th>Disable the application on DR DSR servers.</th>
<th>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 &amp; 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>SSH to physical IP address of the designated primary DR DSR as root and make it primary</td>
<td>1. Login via SSH to the physical IP of the chosen primary DR DSR server as root user. 2. Execute the command <code>top.setPrimary</code> 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.</td>
</tr>
<tr>
<td>3</td>
<td>Verify replication</td>
<td>1. Monitor [Main Menu: Status &amp; 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.’</td>
</tr>
<tr>
<td>4</td>
<td>Re-enable the application on the now-Primary DSR using the Active new-Primary DSR GUI.</td>
<td>1. Login to new-Primary DSR GUI as one of the admin user. 2. Select [Main Menu: Status &amp; 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Decrease the durability admin status and then reconfigure and reconnect the customer’s provisioning clients.</td>
<td></td>
</tr>
</tbody>
</table>
|   | 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.  
|   | 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disable the application on currently Active DSR servers.</td>
</tr>
<tr>
<td>2</td>
<td>Convert former Primary DSR servers to new DR DSR</td>
</tr>
<tr>
<td>3</td>
<td>Start software on newly DR Site</td>
</tr>
<tr>
<td>4</td>
<td>SSH to VIP address of the to-be-primary DSR as root and make it primary</td>
</tr>
</tbody>
</table>

**Disabling 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.
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.

**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.
4. It may take several minutes for replication, afterward the DB and Reporting Status columns should show ‘Normal.’

**Start software on newly DR Site:**

1. Login to new-DR DSR GUI physical IP as one of the admin user.
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.

**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.
## 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.
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.

## 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
```

## 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

## 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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Associated PR</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inetmerge alarm after force restore</td>
<td></td>
<td>Get the clusterID of the NO using the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># top.myrole</td>
</tr>
<tr>
<td></td>
<td></td>
<td>myNodeId=A3603.215</td>
</tr>
<tr>
<td></td>
<td></td>
<td>myMasterCapable=true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>222826</td>
<td>Then update the clusterId field in RecognizedAuthority table to have the same clusterid:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># ivi RecognizedAuthority</td>
</tr>
<tr>
<td>Incorrect NodeID</td>
<td>222826</td>
<td>Restart the Inetrep service on all affected servers using the following commands:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># pm.set off inetrep</td>
</tr>
<tr>
<td></td>
<td></td>
<td># pm.set on inetrep</td>
</tr>
<tr>
<td>Inetrep alarm after performing disaster recovery</td>
<td>222827</td>
<td>Restart the Inetsync service on all affected servers using the following commands:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># pm.set off inetsync</td>
</tr>
<tr>
<td></td>
<td></td>
<td># pm.set on inetsync</td>
</tr>
<tr>
<td>Inetsync alarms after performing disaster recovery</td>
<td>222828</td>
<td>Release 5.X:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>From the recovered NO server command line, execute:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># AppWorks AppWorks_AppWorks updateServerAliases &lt;NO Host Name&gt;</td>
</tr>
<tr>
<td>Active NO /etc/hosts file does not contain server aliases after force restore done</td>
<td>222829,234357</td>
<td>Release 4.X:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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)</td>
</tr>
</tbody>
</table>
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