Oracle® Communications Diameter Signaling Router Full Address Resolution

SDS 8.4 Disaster Recovery User's Guide

Release 8.4

F12362-01

April 2019

Oracle® Communications Diameter Signaling Router Full Address Resolution, SDS 8.4 Disaster Recovery User's Guide, Release 8.4

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.
Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

My Oracle Support (MOS) (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.

See more information on MOS in the Appendix section.

TABLE OF CONTENTS

1.0 INTRODUCTION 6
1.1 Purpose and Scope 6
1.2 References 6
1.3 Acronyms 7
1.4 Assumptions 7
1.5 How to use this Document 7
2.0 DISASTER RECOVERY SCENARIOS 8
2.1 Complete connectivity loss of Primary SDS NOAM Servers 8
2.1.1 Pre Condition 8
2.1.2 Recovery Steps 8
2.1.3 Post Condition 8
2.2 Replacement of a DP server 9
2.2.1 Pre Condition 9
2.2.2 Recovery Steps 9
2.2.3 Post Condition 10
2.3 Replacement of a SOAM Server 11
2.3.1 Pre Condition 11
2.3.2 Recovery Steps 11
2.3.3 Post Condition 12
2.4 Replacement of a Query server 13
2.4.1 Pre Condition 13
2.4.2 Recovery Steps 13
2.4.3 Post Condition 14
2.5 Replacement of a SDS NOAM Server 15
2.5.1 Pre Condition 15
2.5.2 Recovery Steps 15
2.5.3 Post Condition 16
2.6 Replacement of Primary SDS NOAM Server pair 17
2.6.1 Pre Condition 17
2.6.2 Recovery Steps 17
2.6.3 Post Condition 20
2.7 Replacement of SOAM server pair 21
2.7.1 Pre Condition 21
2.7.2 Recovery Steps 21
2.7.3 Post Condition 22
2.8 Replacement of DR SDS NOAM Server pair 23
2.8.1 Pre Condition 23
2.8.2 Recovery Steps 23
2.8.3 Post Condition 24
2.9 Replacement of SDS frame 25
2.9.1 Pre Condition 25
2.9.2 Recovery Steps 25
2.9.3 Post Condition 25
2.10 Replacement of SOAM frame 26
2.10.1 Pre Condition 26
2.10.2 Recovery Steps 26
2.10.3 Post Condition 26
2.11 Replacement of a Failed 4948/4948E/4948E-F Switch (RMS System, No PMAC Installed) (netConfig) 26
2.11.1 Pre Condition 26
2.11.2 Recovery Steps 27
2.11.3 Post Condition 37

APPENDIX A: MY ORACLE SUPPORT (MOS) 38
APPENDIX B: INSTALL NETBACKUP CLIENT 39
APPENDIX C: RESTORE PROVISIONING DATABASE 40
APPENDIX D: RECOVER PDBRELAY 45
APPENDIX E: BACKUP DIRECTORY 46

List of Tables

Table 1 - Acronyms 7

1.0 INTRODUCTION

1.1 Purpose and Scope

This document describes procedures to use during disaster scenarios related to SDS 8.4 product.

The disaster scenarios covered in document are:

1. Connectivity loss to Primary SDS NOAM Servers and DR SDS site activation.
2. A defective DP server
3. A defective Query Server
4. A defective SOAM server
5. A defective SDS NOAM Server
6. A defective SDS NOAM Server pair
7. A defective SOAM server pair
8. A defective CISCO switch
9. Total loss of SDS frame.
10. Total loss of SOAM frame.

This document is intended for execution by My Oracle Support (MOS) on fielded SDS systems.

It also could be used at Oracle by PV and development team.

1.2 References

External *(Customer Facing)**:***

[1] SDS Initial Installation Guide
[2] TPD Initial Product Manufacture, Software Installation Procedure
[3] Oracle@ Communication Tekelec Platform Configuration Guide
[4] DSR 3-Tier Disaster Recovery Guide
[5] DSR Disaster Recovery Guide
[6] DSR / SDS 8.x NOAM Failover User's Guide
[7] Cabinet Assembly Instructions, 910-6083-001

1.3 Acronyms

Acronym	Meaning
CSV	Comma Separated Values
DP	Database Processor
IMI	Internal Management Interface
ISL	Inter-Switch-Link
MP	Message Processor
NE	Network Element
NOAM	Network Operations, Administration & Maintenance
OAM	Operations, Administration & Maintenance
SDS	Subscriber Data Server
RMM	Remote Management Module
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution (Linux OS)
VIP	Virtual IP
XMI	External Management Interface

Table 1 - Acronyms

1.4 Assumptions

This procedure assumes the following;

- The user conceptually understands the topology of SDS and the network configuration.
- The user has at least an intermediate skill set with command prompt activities on an open systems computing environment such as Linux or TPD.

1.5 How to use this Document

When executing this document, understanding the following helps to ensure that the user understands the manual's intent:

1) Before beginning a procedure, completely read the instructional text (it appears immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
2) Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.

If a procedural step fails to execute successfully, then please STOP and contact My Oracle Support (as described in **Appendix A**:).

2.0 DISASTER RECOVERY SCENARIOS

!!WARNING!!

Whenever there is need to restore the database backup for NOAM and SOAM servers in any of below Recovery Scenarios, the backup directory may not be there in the system as system will be DRed.

In this case, refer to Appendix E:: Backup directory, this will provide steps to check and create the backup directory.

2.1 Complete connectivity loss of Primary SDS NOAM Servers

2.1.1 Pre Condition

- User cannot access Primary SDS site GUI
- User can access DR SDS GUI
- Provisioning clients are disconnected from the primary SDS
- Provisioning has stopped

2.1.2 Recovery Steps

In order to quickly make SDS GUI accessible and provisioning to continue, Follow the below instructions:

1. Promoting the DR NOAM from Secondary to Primary follow reference [6]
2. Recover Primary NOAM as DRNO follow reference [6]

Note: The Active Network server allows SNMP administration. Global SNMP configuration cannot be modified if DR site is made Primary. It can be updated once original site becomes Primary again.

2.1.3 Post Condition

- GUI on the new Primary SDS is accessible
- Provisioning clients are connected to the new Primary SDS
- Database provisioning resumes
- A new DR SDS GUI is accessible
- Replication and collection alarms have cleared

NOTE: To swap new Primary SDS and new DR SDS sites back to their original roles, execute Step 8 on new-Primary SDS (old-DR SDS) and step 2 on new-DR SDS (old-Primary SDS) from Procedure 1 (Demoting the Active NOAM from Primary to Secondary) in refernce [6].

2.2 Replacement of a DP server

2.2.1 Pre Condition

- DP server has stopped processing traffic
- It has been determined the DP server is defective and needs replacement
- New DP server is available

2.2.2 Recovery Steps

STEP #	Procedure	Description
1 ☐	Prepare the defective DP server for the replacement.	Identify the defective DP server that needs to be replaced Defective DP server hostname = _____
2 ☐	Stop the application on the defective DP server.	1. Using VIP address, login to SOAM GUI site where defective DP server is located. 2. Navigate to GUI screen [**Main Menu: Status & Manage → Server**] 3. Select the defective DP server by its hostname. 4. Click the 'Stop' button followed by the 'Ok' button on confirmation screen.
3 ☐	Verify that no signaling traffic is processed at the defective DP server	1. Go to [**Main Menu: Status & Manage --> KPIs**] screen. 2. Click the KPI Filter icon on the right edge of the screen. 3. Select "DP" for Group and click the GO dialogue button. 4. Select the tab of the DP server to be recovered. 5. Verify that the "Total Queries/Sec" KPI is now showing "0" for this DP.
4 ☐	Power down the defective DP server.	Power down the defective DP server. **Note:** If HW replacement is deemed necessary, physically remove defective DP blade and install new replacement blade 1. Power down the defective DP server. 2. Label all cables connected to defective DP server. 3. Physically remove defective DP server from the frame. 4. To install the new DP blade use below step from reference [7] - Upgrade firmware on the Blade - Upgrade the BIOS of the blade - Set the iLO credentials userid/password of the blade 5. Power up the new DP server.
5 ☐	Install SDS application on the new DP server	Execute procedure 10, steps 1 through 22 (DP Installation) as described in reference [1]
6 ☐	Configure the new DP server	Execute procedure 10, steps 38 - 65 (Applying TKLCConfigData.sh file on the new DP server) as described in reference [1].
7 ☐	Disable hyperthreading on the new DP server	Execute steps as described in Appendix I (Disable Hyperthreading) from [1].

STEP #	Procedure	Description
8 ☐	Restart the application on the new DP server	Execute procedure 10, steps 86 through 91 (Restarting the application on the new DP server) as described in reference [1]
9 ☐	Verify status and traffic.	1. Go to [Main Menu: Status & Manage --> KPIs] screen. 2. Click the KPI Filter icon on the right edge of the screen. 3. Select "DP" for Group and click the GO dialogue button. 4. Select the tab of the DP server to be recovered. 5. Verify that the "Total Queries/Sec" KPI now showing a non-zero value for this DP
10 ☐	Verify comAgent connections	**1.** Navigate to GUI Screen **[Main Menu: Communication Agent --> Maintenance --> Connection Status].** 2. Verify comAgent connections (Automatic & Configured).

2.2.3 Post Condition

- DP server is processing traffic

2.3 Replacement of a SOAM Server

2.3.1 Pre Condition

- SOAM server has stopped functioning
- It has been determined to replace the blade hosting SOAM server
- New blade replacement is available
- SDS GUI is accessible

2.3.2 Recovery Steps

STEP #	Procedure	Description
1 ☐	Prepare for server replacement.	Identify the SOAM server that needs replacement Defective SOAM server hostname = _____
2 ☐	Make SOAM server's Max Allowed HA Role "Standby" so it does not become active.	1. Login to the Primary SDS NOAM GUI as admin user using VIP address. 2. Navigate to GUI screen [**Main Menu: Status & Manage → HA**] 3. Click 'Edit' button 4. Change "Max Allowed HA Role" of the defective SOAM server to 'Standby' 5. Click OK button
3 ☐	Remove SOAM server from the server group.	1. Navigate to GUI screen [**Main Menu: Configuration → Server Groups**]. 2. Select SOAM's server group. 3. Click the "Edit" button. 4. Under "SG Inclusion", uncheck the defective SOAM server. 5. Click the "OK" button.
4 ☐	Replace hardware and Recover DSR services	Replace OAM blade hardware and restore TVOE network configuration in accordance with the DSR Disaster Recovery Guide [5].
5 ☐	Add SDS Software Images to PMAC Servers	Execute Procedure 7, steps 1 through 15 (Add SDS Software Images to PMAC Servers) from reference [1].
6 ☐	Install SDS application on he new SOAM server	Execute Procedure 8, steps 1 through 22 (Installing the SDS Application) from reference [1].
7 ☐	Prepare the new SOAM server	Execute Procedure 8, steps 45 through 74 (Applying TKLCConfigData.sh file on the new SOAM server) from reference [1].
8 ☐	Add the new SOAM server back to the server group	Execute procedure 9, steps 14 through 20 (Adding new SOAM server back to the Server Group) from reference [1].
9 ☐	Restart the application on the new SOAM server	Execute procedure 9, steps 26 through 32 (Restarting application on new SOAM server) from reference [1].

2.3.3 Post Condition

- SOAM server is back in the service

2.4 Replacement of a Query server

2.4.1 Pre Condition

- Query server has stopped functioning
- It has been determined to replace the Query server
- New Query server replacement is available

2.4.2 Recovery Steps

STEP #	Procedure	Description
1 ☐	Prepare for Query server replacement.	Identify the defective Query server that needs replacement Defective Query server hostname = _____
2 ☐	Remove the defective Query Server from the server group.	1. Go to the SDS GUI. 2. Navigate to GUI screen [**Main Menu: Configuration → Server Groups**] 3. Select Query Server's server group. 4. Click the "Edit" button. 5. Under "SG Inclusion", uncheck the defective Query server. 6. Click the "OK" button.
3 ☐	Power down and replace Query Server	1. Power down the defective Query server. 2. Label all cables connected to the defective Query server. 3. Physically remove the defective Query server from the frame 4. All connections should be made to the replacement server according to the labels attached in **sub-step 2** of the same step 5. Power up the new Query server 6. To install the new Query Server use below step from reference [7] - check/upgrade firmware on the Blade - upgrade the BIOS of the blade - set the iLO credentials userid/password of the blade
4 ☐	Install SDS application on the new Query server	Execute Procedure 1 (Installing the SDS Application on the new Query server) as described in reference [1].
5 ☐	Prepare the new Query server	Execute procedure 4, steps 17 through 43 (Applying TKLCConfigData.sh file on the new Query server) as described in reference [1].
6 ☐	Add the new Query server back to SDS NOAM Server group	Execute procedure 4, steps 44 through 50 (Adding query server back to SDS NOAM Server group) as described in reference [1].
7 ☐	Restart the application on the new Query server	Execute procedure 4, steps 51 through 56 (Restarting SDS application on the query server) as described in reference [1].

2.4.3 Post Condition

- Query server is back in service

2.5 Replacement of a SDS NOAM Server

2.5.1 Pre Condition

- SDS NOAM Server has stopped functioning
- It has been determined to replace the defective SDS NOAM Server
- New SDS NOAM Server replacement is available

2.5.2 Recovery Steps

STEP #	Procedure	Description
1 ☐	Prepare for server replacement.	Identify the defective SDS NOAM Server that needs replacement Defective SDS NOAM Server hostname = _____
2 ☐	Make the defective SDS NOAM Server "Standby" so it does not become active.	1. Login to the Primary SDS GUI as admin user using VIP address. 2. Navigate to GUI screen [**Main Menu: Status & Manage → HA**] 3. Click 'Edit' button 4. Change "Max Allowed HA Role" of the defective SDS NOAM Server to 'Standby' 5. Click OK button
3 ☐	Remove SDS NOAM Server from the server group.	1. Navigate to GUI screen [**Main Menu: Configuration → Server Groups**] 2. Select SDS's server group. 3. Click the "Edit" button. 4. Under "SG Inclusion", uncheck the defective SDS NOAM Server 5. Click the OK button.
4 ☐	Power down and replace SDS NOAM Server	1. Power down the defective SDS NOAM Server. 2. Label all cables connected to the defective SDS NOAM Server. 3. Physically remove the defective SDS NOAM Server from the frame 4. All connections should be made to the replacement server according to the labels attached in **sub-step 2** of the same step. 5. Power up the new SDS NOAM Server 6. To install the new NOAM Server use below step from reference [7] - check/upgrade firmware on the Blade - upgrade the BIOS of the blade - set the iLO credentials userid/password of the blade
5 ☐	Install the SDS application on new SDS NOAM Server	Execute Procedure 1 (Installing the SDS Application) from reference [1].
6 ☐	Prepare SDS NOAM Server	Execute procedure 2, steps 26 through 49 , then Steps 52-55. (Applying TKLCConfigData.sh file on the new SDS NOAM Server) from reference [1].
7 ☐	Add the new SDS NOAM Server back to the server group	Execute procedure 3, steps 1, 13 through 25 (Pairing SDS NOAM Servers) from reference [1].

STEP #	Procedure	Description
8 ☐	Restart the application on new SDS NOAM Server	Execute procedure 3, steps 26 through 40 (Paring the SDS NOAM Servers SDS NOAM Server) from reference [1].
9 ☐	Re-exchange SSH keys for Remote Import, Remote Export, and Data Export features	1. Login to the Primary SDS GUI as admin user using VIP address. 2. Perform SSH key exchange for Remote Export using this screen [**Main Menu: SDS → Configuration → Options**] 3. Perform SSH key exchange for Remote Import using this screen [**Main Menu: SDS → Configuration → Options**] 1. Perform SSH key exchange for Data Export using this screen [**Main Menu: Administration → Remote Servers → Data Export**]
10 ☐	Install Netbackup Client Software (optional)	1. Execute steps as described in Appendix B:

2.5.3 Post Condition

- SDS NOAM Server is back in service

2.6 Replacement of Primary SDS NOAM Server pair

2.6.1 Pre Condition

- Primary SDS-A, Primary SDS-B, and Primary SDS Query servers have stopped functioning
- DR SDS NOAM Servers are NOT available or are NOT installed
- It has been determined to replace Primary SDS NOAM Servers
- New Primary SDS NOAM Servers for replacement are available
- Recent backup archives of SDS configuration and provisioning databases are available

NOTE: If DR SDS NOAM Servers are available, then follow recovery steps from Section 2.1 of this document

2.6.2 Recovery Steps

STEP #	Procedure	Description

1 ☐	Determine SDS backup archive files	Make sure that you have access to SDS Configuration and Provisioning backup archive files
		
		Configuration backup archive file
		_____
		Provisioning backup archive file
		_____
		
		1. Note: The backup archive files should be in uncompressed format.
		If it is not uncompress then please execute following commands.
		
		For gunzip file:
		$ gunzip Backup.sds.sds1-noa-1191038.Configuration.NETWORK_OAMP.20160609_021511.AUTO.tar.gz
		
		$ gunzip Backup.sds.sds1-noa-1191038.Provisioning.NETWORK_OAMP.20160609_021511.AUTO.tar.gz
		
		For bunzip file:
		$ bunzip2 Backup.sds.sds1-noa-1191038.Configuration.NETWORK_OAMP.20160609_021511.AUTO.tar.bz2
		
		$ bunzip2 Backup.sds.sds1-noa-1191038.Provisioning.NETWORK_OAMP.20160609_021511.AUTO.tar.bz2

STEP #	Procedure	Description
2 ☐	Power down and remove all defective Primary SDS NOAM Servers. Replace them with new SDS NOAM Servers.	1. Power down all defective SDS NOAM Servers. 2. Label all cables connected to defective SDS NOAM Servers. 3. Physically remove defective SDS NOAM Servers from the frame. 4. Follow reference [7] for the physical installation of new SDS NOAM Servers. 5. Wire in the new SDS NOAM Servers according to the cables you labeled and removed from the old servers. 6. To install the new NOAM Server use below step from reference [7] - check/upgrade firmware on the Blade - upgrade the BIOS of the blade - set the iLO credentials userid/password of the blade
3 ☐	Install the SDS application on the new Primary SDS-A server	Execute Procedure 1 on the new Primary SDS-A server (Installing the SDS Application) from reference [1].
4 ☐	Configure temporary IP address	Configure temporary external IP address on the new Primary SDS-A server, as described in Appendix C of [1].
5 ☐	Copy SDS backup archive files to the new Primary SDS-A server.	1. Login via SSH to the console of the new Primary SDS-A server. 2. Execute following commands on console: **sudo su -** **cd /var/TKLC/db/filemgmt** **mkdir backup** **chown awadmin:awadm backup** **chmod 775 backup** 3. Copy the uncompressed backup archive files identified in step 1 to **/var/TKLC/db/filemgmt/backup** area on newly installed Primary SDS-A server. 4. Execute this command to stop running applications. Leave database running. **# prod.stop** 5. Restore the configuration DB by executing this command **# idb.restore -n -t /var/TKLC/db/filemgmt/backup/ -v <full path to configuration archive file name>** 6. SDS database is now restored. Start application by executing **# prod.start** 7. Exit out of root: **# exit**
6 ☐	Prepare the new Primary SDS-A server	Execute procedure 2, steps 26 through 49 and steps 53 through 55 on the new Primary SDS-A server (Applying TKLCConfigData.sh file) from reference [1].

STEP #	Procedure	Description
7 ☐	Install the SDS application on the new Primary SDS-B server	Execute Procedure 1 on the new Primary SDS-B server (Installing the SDS Application) from reference [1].
8 ☐	Prepare the new Primary SDS-B server	Execute procedure 2, steps 26 through 49 and steps 53 through 56 on the new Primary SDS-B server (Applying TKLCConfigData.sh file) from reference [1].
9 ☐	Restore Provisioning Database	Follow steps in **Appendix C**.
10 ☐	Install the SDS application on the new Primary SDS Query server	To install the new Query Server use below step from reference [1] - check/upgrade firmware on the Blade - upgrade the BIOS of the blade - set the iLO credentials userid/password of the blade Execute Procedure 1 on the new Primary SDS Query server (Installing the SDS Application) from reference [1].
11 ☐	Prepare the new Primary SDS Query server	Execute procedure 4, steps 17 through 43 and steps 52 through 57 on the new Primary SDS Query server (Applying TKLCConfigData.sh file) from reference [1].
12 ☐	Restart the application on all new Primary SDS NOAM Servers	1. Login to the Primary SDS GUI as admin user using VIP address 2. Navigate to GUI screen [**Main Menu: Status & Manage → Server**] 3. Select the Primary SDS-A server 4. Click the “Restart” button 5. In pop-up window, click the “OK” button to confirm Repeat all above for Primary SDS-B server, and Primary SDS Query server
13 ☐	Install Netbackup Client Software on Primary SDS-A and Primary SDS-B servers (optional)	Execute steps as described in Appendix B:
14 ☐	Re-exchange SSH keys for Remote Import, Remote Export, and Data Export features	1. Login to the Primary SDS GUI as admin user using VIP address. 2. Perform SSH key exchange for Remote Export using this screen [**Main Menu: SDS → Configuration → Options**] 3. Perform SSH key exchange for Remote Import using this screen [**Main Menu: SDS → Configuration → Options**] 4. Perform SSH key exchange for Data Export using this screen [**Main Menu: Administration → Remote Servers → Data Export**]

2.6.3 Post Condition

- Primary SDS-A, Primary SDS-B, and Primary SDS Query servers are back in service
- Provisioning clients are connected to SDS VIP address
- Provisioning continues

2.7 Replacement of SOAM server pair

2.7.1 Pre Condition

- Both SOAM-A and SOAM-B servers have stopped functioning
- It has been determined to replace both blades that host SOAM servers
- New blades for replacement are available
- Access to Primary SDS GUI is available
- DPs are not receiving provisioning database updates.

2.7.2 Recovery Steps

STEP #	Procedure	Description
1 ☐	Prepare for server replacement.	Identify the SOAM-A and SOAM-B servers that needs replacement SOAM-A Server: _____ SOAM-B Server: _____ SOAM Network Element name _____
2 ☐	Inhibit database replication for defective SOAM servers and DP servers associated with this SOAM network element. **NOTE**: It is expected that each SOAM and subtending DP will have a DB Level of "UNKNOWN" until the SOAMs are restored.	1. Go to the NOAMP GUI. 2. Select [**Main Menu: Status & Manage → Database**] screen 3. Filter on the SOAM Network Element name. 4. Record the DP server hostnames (Role: MP). 5. Click “Inhibit Replication” button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited 6. "Inhibiting" SOAM server: Click “Inhibit Replication” button for each defective SOAM servers identified in the above step 1
3 ☐	Remediate OAM blade hardware and restore TVOE network configuration.	Remediate OAM blade hardware and restore TVOE network configuration in accordance with the DSR Disaster Recovery Guide [5].
4 ☐	Install SDS application on the new SOAM-A server	Execute Procedure 8, steps 1 through 22 (Installing the SDS Application on SOAM server) from reference [1].

5 ☐	Install SDS application on the new SOAM-B server	Execute Procedure 8, steps 1 through 22 (Installing the SDS Application on SOAM server) from reference [1].
6 ☐	Prepare the new SOAM-A server	Execute Procedure 8, steps 45 through 76 (Applying TKLCConfigData.sh file on SOAM server) from reference [1].
7 ☐	Prepare the new SOAM-B server	Execute Procedure 8, steps 45 through 48, 50 through 70 and 72 through 76 (Applying TKLCConfigData.sh file on SOAM server) from reference [1].
8 ☐	Allow database replication for SOAM-A and SOAM-B servers and DP servers associated with this SOAM network element.	1. Go to the NOAMP GUI. 2. Select [**Main Menu: Status & Manage** → **Database**] screen 3. Filter on the SOAM Network Element name. 4. Record the DP server hostnames (Role: MP). 5. Allowing Replication: Click “Allow Replication” button for each newly replaced SOAM-A and SOAM-B servers 6. Wait until audit becomes active on SOAM's. Allowing Replication: Click “Allow Replication” button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited
9 ☐	Restart the application on the new SOAM-A server	Execute procedure 9, steps 26 through 32 (Restarting application on SOAM server) from reference [1].
10 ☐	Restart the application on the new SOAM-B server	Execute procedure 9, steps 26 through 29 and 33 through 35 (Restarting application on SOAM server) from reference [1].
11 ☐	Verify that SOAM servers receive SDS provisioning	1. Login to active SOAM GUI using VIP address. 2. Select [**Main Menu: Status & Manage** → **Servers**] screen. 3. Make sure that new SOAM servers show ‘Norm’ for DB, Reporting Status and Appl State.
12 ☐	Verify that SOAM servers showng valid DB level	1. Go to the SOAM GUI. 2. Select [**Main Menu: Status & Manage** → **Database**] screen 3. Verify that a valid DB Level is now showing for each SOAM and subtending DP.

2.7.3 Post Condition

- Both SOAM servers are back in service
- DPs are now receiving provisioning updates

2.8 Replacement of DR SDS NOAM Server pair

2.8.1 Pre Condition

- DR SDS-A, DR SDS-B, and DR SDS Query servers have stopped functioning
- It has been determined to replace DR SDS NOAM Servers
- New DR SDS NOAM Servers for replacement are available
- Access to Primary SDS GUI is functional

2.8.2 Recovery Steps

STEP #	Procedure	Description
1 ☐	Prepare for server replacement.	Identify the DR SDS NOAM Servers that needs replacement DR SDS-A Server: _____ DR SDS-B Server: _____ DR SDS Query Server: _____
2 ☐	Power down and remove all defective DR SDS NOAM Servers. Replace them with new servers.	1. Power down all defective DR SDS NOAM Servers. 2. Label all cables connected to defective DR SDS NOAM Servers. 3. Physically remove defective DR SDS NOAM Servers from the frame. 4. Wire in the new DR SDS NOAM Servers according to the cables you labeled and removed from the old servers. 5. To install the new DR SDS NOAM Server use below step from reference [1] - check/upgrade firmware on the Blade - upgrade the BIOS of the blade - set the iLO credentials userid/password of the blade.
3 ☐	Install the SDS application on the new DR SDS-A server	Execute Procedure 1 on the new DR SDS-A server (Installing the SDS Application) from reference [1].
4 ☐	Prepare the new DR SDS-A server	Execute procedure 5, steps 22 through 45 on the new DR SDS-A server (Applying TKLCConfigData.sh file) from reference [1]. And then execute Procedure 6, steps 26 through 32 (Restarting application on DR SDS NOAM server) from reference [1].
5 ☐	Install the SDS application on the new DR SDS-B server	Execute Procedure 1 on the new DR SDS-B server (Installing the SDS Application) from reference [1].
6 ☐	Prepare the new DR SDS-B server	Execute procedure 5, steps 22 through 45 on the new DR SDS-B server (Applying TKLCConfigData.sh file) from reference [1]. And then execute Procedure 6, steps 26 through 32 (Restarting application on DR SDS NOAM server) from reference [1].
7 ☐	Install the SDS application on the new DR SDS Query server	Execute Procedure 1 on the new DR Query server (Installing the SDS Application) from reference [1].

8 ☐	Prepare the new DR SDS Query server	Execute procedure 4, steps 17 through 43 on the new Query server (Applying TKLCConfigData.sh file) from reference [1] and then execute Procedure 4 (Configuring the Query Server), steps 54 through 56 (Restarting application on DR SDS Queryserver) from reference [1].
9 ☐	Verify DB level	Navigate to the **[Main Menu: Status & Manage --> Database]** screen to verify that a valid DBLevel is now showing for each DR NOAM and DR site Query Server. NOTE: Any value except "UNKNOWN" and "0" is valid for DB level.
10 ☐	Install Netbackup Client Software on DR SDS-A, and DR SDS-B servers (optional)	Execute steps as described in Appendix B:
11 ☐	Re-exchange SSH keys for Remote Import, Remote Export, and Data Export features	1. Login to the Primary SDS GUI as admin user using VIP address. 2. Perform SSH key exchange for Remote Export using this screen [**Main Menu: SDS → Configuration → Options**] 3. Perform SSH key exchange for Remote Import using this screen [**Main Menu: SDS → Configuration → Options**] 4. Perform SSH key exchange for Data Export using this screen [**Main Menu: Administration → Remote Servers → Data Export**]

2.8.3 Post Condition

- All DR SDS NOAM Servers are back in service

2.9 Replacement of SDS frame

2.9.1 Pre Condition

- SDS frame is destroyed
- A replacement SDS frame with 2 SDS NOAM Servers and a Query Server is available
- DR SDS NOAM Servers are available
- Access to DR SDS GUI is functional

2.9.2 Recovery Steps

STEP #	Procedure	Description
1 ☐	Determine SDS site and status of provisioning	If the destroyed SDS frame was the Primary SDS frame, then execute procedure from refenrece [6] to activate DR SDS site as a new Primary SDS site. This allows provisioning to continue and makes the defective frame as a defective DR SDS frame.
2 ☐	Install new replacement DR SDS frame	Follow reference [2] to install new DR SDS frame.
3 ☐	Install DR SDS NOAM Servers in new DR SDS frame	Install new DR SDS NOAM Servers into new DR SDS frame by following instructions in reference [7].
4 ☐	Install switches in new DR SDS frame	Install new switches into new DR SDS frame by following instructions in reference [7]
5 ☐	Connect DR SDS NOAM Servers	Wire in the new DR SDS NOAM Servers by following instructions in reference[7].
6 ☐	Recover DR SDS NOAM Server pair	Follow recovery steps from **Section 2.8** of this document.
7 ☐	Recover Query server	Follow recovery steps from **Section 2.4** of this document.

2.9.3 Post Condition

- DR SDS frame is back in the service

2.10 Replacement of SOAM frame

2.10.1 Pre Condition

- SOAM frame is destroyed
- A replacement SOAM frame with 2 SOAM servers and DP servers is available

2.10.2 Recovery Steps

STEP #	Procedure	Description
1 ☐	Install new SOAM frame	Follow procedures in reference [4]to install new SOAM frame.
2 ☐	Install SOAM Cabinet	Follow reference [5] for installation of HP BladeSystem enclosure.
3 ☐	Install DSR	Execute Recovery Scenario 1, of reference [4], DSR Disaster Recovery Guide, to restore DSR services.
4 ☐	Recover SOAM server pair	Follow recovery steps from **Section 2.7** of this document.
5 ☐	Recover DP servers	For each DP server, follow recovery steps from **Section 2.2** of this document.

2.10.3 Post Condition

- SOAM frame is back in service

2.11 Replacement of a Failed 4948/4948E/4948E-F Switch (RMS System, No PMAC Installed) (netConfig)

This procedures assumes a Platform 7.5 interconnect. If the system being configured follows a different platform interconnect, then the appropriate platform procedures should be followed.

2.11.1 Pre Condition

- A fully configured and operational redundant switch must be in operation. If this is not ensured, connectivity may be lost to the end devices.
- Application username and password for creating switch backups must be configured on the management server before executing this procedure.
- Each switch pair must be configured the same at each SDS deployment
- The xml file packaged with the SDS ISO must be used instead of a switch backup file

2.11.2 Recovery Steps

Recovery steps of Cisco 4948E-F Switch1A for all SDS NOAM sites.

Step	Procedure	Result
1. ☐	**Cabinet**: Power off failed switch	If the failed switch is DC powered, power off using the cabinet breakers, then remove the DC power and ground cables. If the failed switch is AC powered, remove the AC power cords from the unit.
2. ☐	**Cabinet**: Find and prepare to replace switch	Determine whether switch1A or switch1B failed, locate the failed switch, and detach all network and console cables from the failed switch. ***Note***: If needed label cables before removal.
3. ☐	**Cabinet**: Replace switch	Remove failed switch and replace with new switch of same model.
4. ☐	**Cabinet**: Power on replacement switch	If the switch is DC powered, attach the DC power and ground cables, then power on the replacement switch using the appropriate cabinet breakers; otherwise, connect the AC power cords to the unit (AC).
5. ☐	**Cabinet**: Attach cable to new switch	Connect all network and console cables to the new switch. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch.

6. ☐	**SERVER A:**
	Verify the switch netConfig xml files exist of the server
		$ ls -l /usr/TKLC/plat/etc/switch/xml/
		
		Verify the following files are listed:
		
		`DR_switch1A_SDS_4948E_E-F_configure.xml`
		`DR_switch1B_SDS_4948E_E-F_configure.xml`
		`Primary_switch1A_SDS_4948E_E-F_configure.xml`
		`Primary_switch1B_SDS_4948E_E-F_configure.xml`
		`switch1A_SDS_4948E_E-F_init.xml`
		`switch1B_SDS_4948E_E-F_init.xml`
		
		If any file does not exist, contact Customer Care Center for assistance.

Step	Procedure	Result

7. ☐	**Server A**: Determine the IOS image required for the switch.
	
	Note: Both switches must use the same IOS.
		If the appropriate image does not exist, copy the image to the management server.
		Note: Check the FW version on the mate switch and select the matching FW image from the backup directory/TFTP directory.
		To check the FW on the mate switch, use the following command:
		
		If replacing switch1A:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware`
		
		If replacing switch1B:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware`
		
		`Version: 122-54.WO`
		`License: entservicesk9`
		`Flash: cat4500e-entservicesk9-mz.122-54.WO.bin`

8.	**Server A**: Verify IOS image is on system	Determine if the IOS image for the 4948/4948E/4948E-F is on the server: `$ sudo /bin/ls -l /var/lib/tftpboot/<IOS_image_file>` If the file exists and is in the TFTP directory, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media.

9. ☐	**Server A:** Enable tftp on the system for tftp transfer of IOS upgrade file	`$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd startXinetdService service tftp`
		
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`
		`1`

10. ☐	**Server A:** Configure the firewall to allow tftp	`$ sudo iptablesAdm insert --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s 169.254.1.0/24  -p udp --dport 69 -j ACCEPT" --location=1`

Step	Procedure	Result

11. ☐	**Server A:** Verify firewall is configured	`$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter`
		
		`Output:`
		`Persist Domain Table Chain Match`
		`Yes 10platnet filter INPUT -s 169.254.1.0 -p udp –dport 69 -j ACCEPT`

12. ☐	**Server A:** Manipulate the server physical interfaces	Ensure the interface of the server connected to the switch being recovered is the only interface up by performing the following commands:
		
		`$ sudo /sbin/ifup <NIC to switch>`
		`$ sudo /sbin/ifdown <NIC to mate switch>`
		
		If switch1A is being recovered, ensure eth01 is up and eth11 is down.
		
		If switch1B is being recovered, ensure eth11 is up and eth01 is down.

13. ☐	**Server A:** Determine server's management IP address	Obtain the management IP address of the server's management interface (*typically bond0.2*). `$ sudo /sbin/ip addr show bond0.2 | grep inet` The command output should contain the IP address NOAM's management IP address. ***If the IP address is 169.254.1.11 use templates for the Primary Site.*** ***If the IP address is 169.254.1.14 use templates for the DR Site.***

Step	Procedure	Result
14. ☐	**Server A:** Get PROM information	***Note***: ROM and PROM are intended to have the same meaning for this procedure. Connect to the switch and check the PROM version. If replacing switch1A: Connect serially to switch1A by issuing the following command. `$ sudo /usr/bin/console -M <noam_mgmnt_IP_address> -l platcfg switch1A_console` If replacing switch1B: Connect serially to switch1B by issuing the following command. `$ sudo /usr/bin/console -M <noam_mgmnt_IP_address> -l platcfg switch1B_console` `Enter platcfg@pmac5000101's password:` `<platcfg_password>` `[Enter `^Ec?' for help]` `Press Enter` `Switch> show version | include ROM` `ROM: 12.2(31r)SGA1` `System returned to ROM by reload` ***Note***: If the console command fails, contact My Oracle Support (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<Ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in **Appendix G Upgrade Cisco 4948 PROM** of the **Platform Management and Configuration Guide**, **Release 7.6 (E93270-01)**, to upgrade the PROM.

Step	Procedure	Result

15. ☐	**Server A:** Reset switch to factory defaults	Connect serially to the switch and reload the switch by issuing the following commands:
		`Switch>en`
		`Switch#write erase`
		`Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]`
		`[OK]`
		`Erase of nvram: complete`
		`Switch#reload`
		`Proceed with reload? [confirm]`
		
		Wait until the switch reloads, then exit from console; press **<Ctrl-e><c><.>** and you are returned to the server prompt. Wait for the first switch to finish before repeating this process for the second switch.
		Note: There might be messages from the switch. If asked to confirm, press **Enter**. If asked yes or no, type in **no** and press **Enter**.

Step	Procedure	Result

16. ☐	**SERVER A:**
	Initialize switch
		If replacing switch1A, issue the following command:
		`sudo netConfig --file=/usr/TKLC/plat/etc/switch/xml/switch1A_SDS_4948E_E-F_init.xml`
		
		If replacing switch1B, issue the following command:
		`sudo netConfig --file=/usr/TKLC/plat/etc/switch/xml/switch1B_SDS_4948E_E-F_init.xml`
		
		`Sample output from command:`
		`Processing file: =/usr/TKLC/plat/etc/switch/xml/switch1A_SDS_4948E_E-F_init.xml`
		
		Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact My Oracle Support (MOS)
		
		A successful completion of netConfig returns you to the prompt.
		
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.
		For switch1A:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname`
		`Hostname: switch1A`
		
		For switch1B:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname`
		`Hostname: switch1B`
		
		Note: If the correct hostname was not returned the switch was not successfully initialized. Stop this procedure and troubleshoot the issue and/or contact My Oracle Support (MOS)

17. ☐	**SERVER A:**
	Configure the switches
		To determine if Primary or DR templates are to be used, refer to step 12.
		
		If replacing switch1A at the Primary site, issue the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/plat/etc/switch/xml/Primary_switch1A_SDS_4948E_E-F_configure.xml`
		
		If replacing switch1A at the DR site, issue the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/plat/etc/switch/xml/`DR_switch1A_SDS_4948E_E-F_configure.xml
		
		If replacing switch1B at the Primary site, issue the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/plat/etc/switch/xml/Primary_switch1B_SDS_4948E_E-F_configure.xml`
		
		If replacing switch1B at the DR site, issue the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/plat/etc/switch/xml/`DR_switch1B_SDS_4948E_E-F_configure.xml
		
		`Sample Output:`
		`Processing file: /usr/TKLC/plat/etc/switch/xml/`DR_switch1B_SDS_4948E_E-F_configure.xml
		
		Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact My Oracle Support (MOS).
		
		A successful completion of netConfig returns you to the prompt.
		
		Use netConfig to display the configuration of the switch. To verify the switch was configured properly, and to verify netConfig can connect to the switch.
		
		For switch1A:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A showConfiguration`
		
		For switch1B:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B showConfiguration`
		
		Note: The configuration of both switches should be very similar. As a guideline, the configuration of the recovered switch can be compared to the existing configuration of the mate switch.

Step	Procedure	Result

18. ☐	**Server A: :** Verify switch is using proper IOS image per Firmware Release Notes	Verify the switch is using the proper IOS image by issuing the following commands:
		
		For switch1A:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware`
		
		For switch1B:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware`
		
		`Version: 122-54.WO`
		`License: entservicesk9`
		`Flash: cat4500e-entservicesk9-mz.122-54.WO.bin`

19. ☐	**Server A:** Disable TFTP	`$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp force yes`
		
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`
		`1`

20. ☐	**Server A:** Verify TFTP is disabled	Ensure the tftp service is not running by executing the following command:
		
		`A zero is expected.`
		
		`$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd getXinetdService service tftp`
		
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`
		`0`
		
		If a 1 is returned, repeat this step until getXinetdService returns a zero.

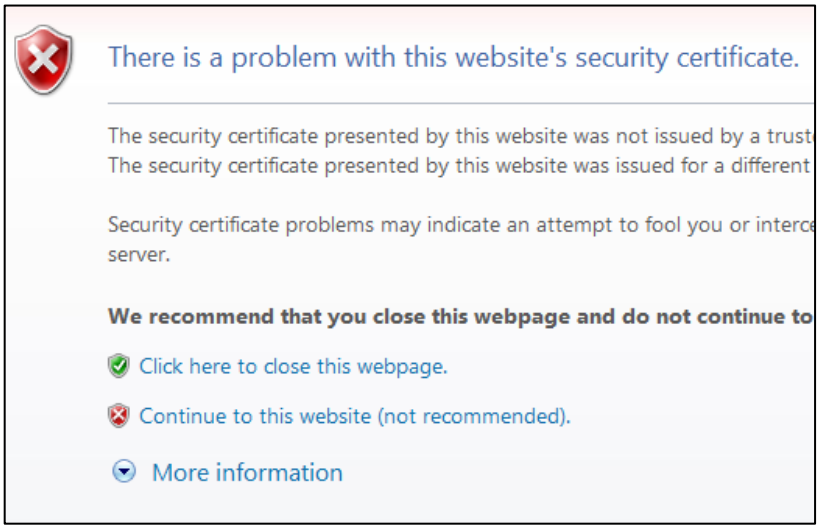
21. ☐	**Server A:** Remove the iptables rule to allow TFTP	`$ sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match "-s 169.254.1.0/24  -p udp --dport 69 -j ACCEPT"`

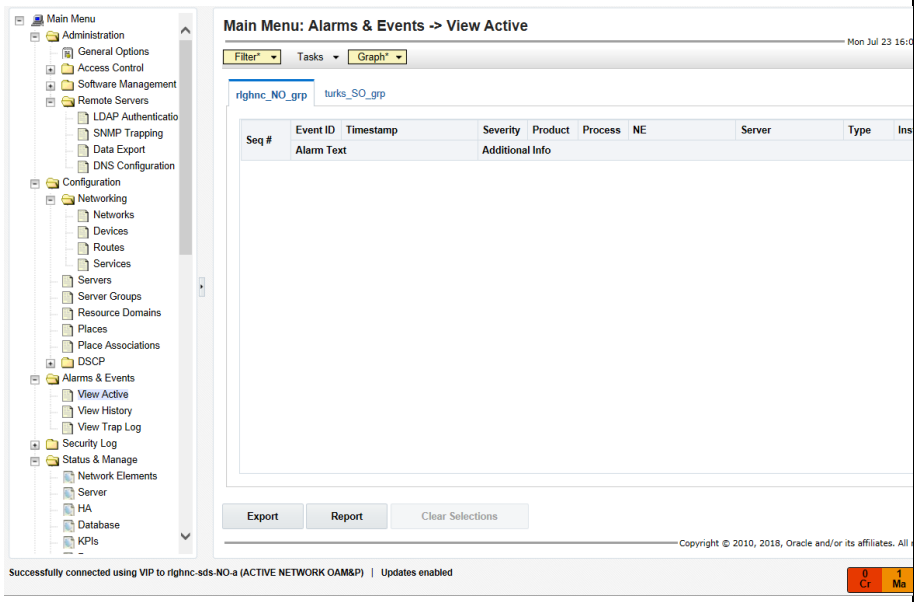
22. ☐	**Server A:** Verify Firewall rules to allow TFTP has been removed.	`$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter`
		
		`Persist Domain  Table  Chain Match`

Step	Procedure	Result
23. ☐	**Server A:** Bring the bond0 interface back up.	Ensure the interface of the server connected to the switch being recovered is the only interface up by performing the following commands: `$ sudo /sbin/ifup <NIC to switch>` ***If switch1A is being recovered, bring eth11 up*** ***If switch1B is being recovered, bring eth01 up.***
24. ☐	**Server A:** Ensure both interfaces of bond0 are up	Ensure the bond0 interfaces are both up by executing the following command: $ sudo cat /proc/net/bonding/bond0 Sample output: [admusr@rlghnc-sds-NO-a ~]$ sudo cat /proc/net/bonding/bond0 Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011) Bonding Mode: fault-tolerance (active-backup) Primary Slave: None Currently Active Slave: eth01 MII Status: up MII Polling Interval (ms): 100 Up Delay (ms): 200 Down Delay (ms): 200 Slave Interface: eth01 MII Status: up Speed: 1000 Mbps Duplex: full Link Failure Count: 3 Permanent HW addr: ac:16:2d:7b:93:f0 Slave queue ID: 0 Slave Interface: eth11 MII Status: up Speed: 1000 Mbps Duplex: full Link Failure Count: 0 Permanent HW addr: ac:16:2d:83:43:67 Slave queue ID: 0 [admusr@rlghnc-sds-NO-a ~]$

Step	Procedure	Result

25. ☐	**Server A:** Verify ping to both switches	Ping each of the switches' SVI (router interface) addresses to verify switch configuration.
		`$ /bin/ping 169.254.1.1`
		`$ /bin/ping 169.254.1.2`

26. ☐	**Primary SDS VIP:** Launch an approved web browser and connect to the XMI Virtual IP Address (VIP) of the Active SDS site **NOTE:** *If presented with the "security certificate" warning screen shown to the right, choose the following option:* ***"Continue to this website (not recommended)".***	
27. ☐	**Primary SDS VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

Step	Procedure	Result
28. ☐	**SDS VIP:** Select… **Main Menu** **→ Alarms & Events** **→ *View Active*** …as shown on the right. Verify no alarms are exits that are reporting device interface or replication issues.	
THIS PROCEDURE HAS BEEN COMPLETED		

2.11.3 Post Condition

- The switch 4948 is replaced and back in service

APPENDIX A: MY ORACLE SUPPORT (MOS)

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs.

A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the United States), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.

When calling, there are multiple layers of menu selections.

Make the selections in the sequence shown below on the Support telephone menu:

1. For the first set of menu options, select:

   2, “New Service Request”.

   You will hear another set of menu options.

2. In this set of menu options, select:

   3, “Hardware, Networking and Solaris Operating System Support”.

   A third set of menu options begins.

3. In the third set of options, select:

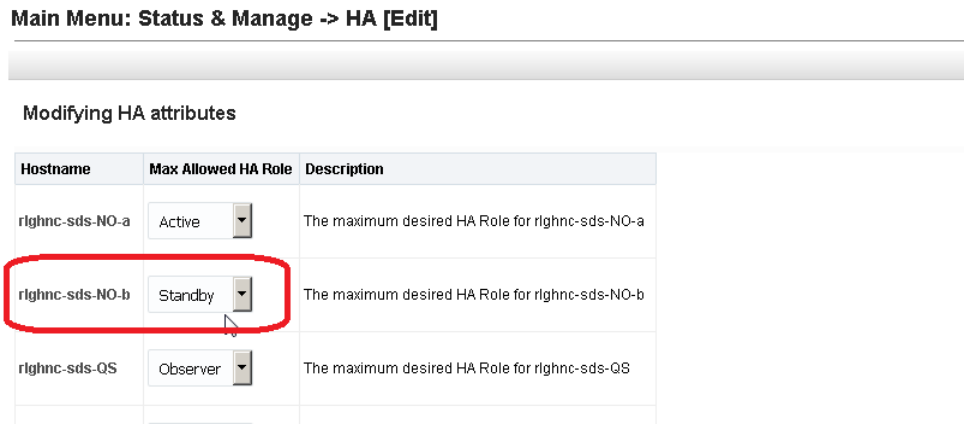
   2, “ Non-technical issue”.

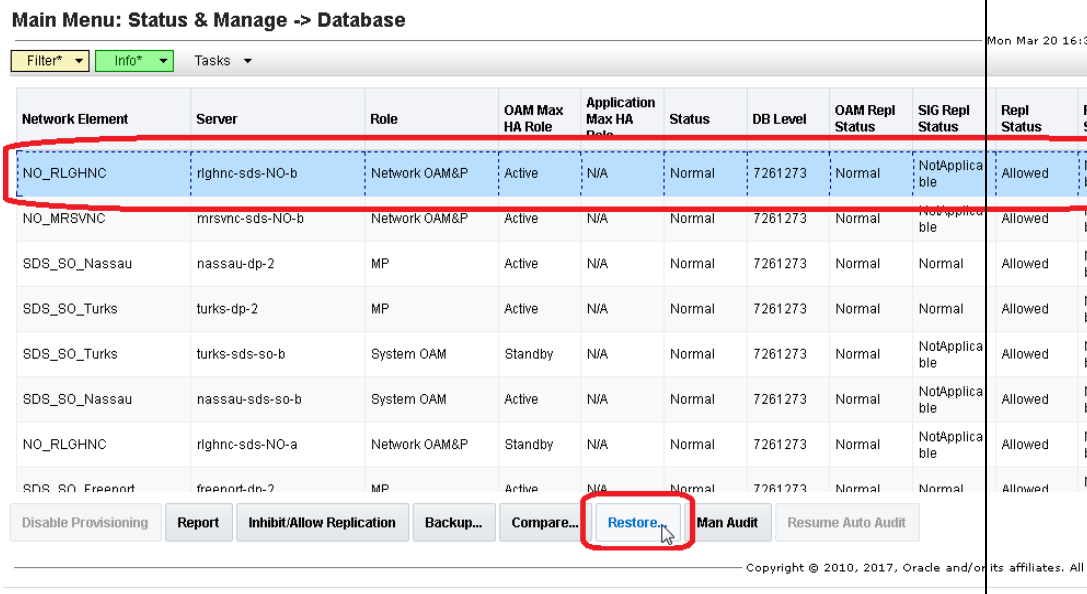
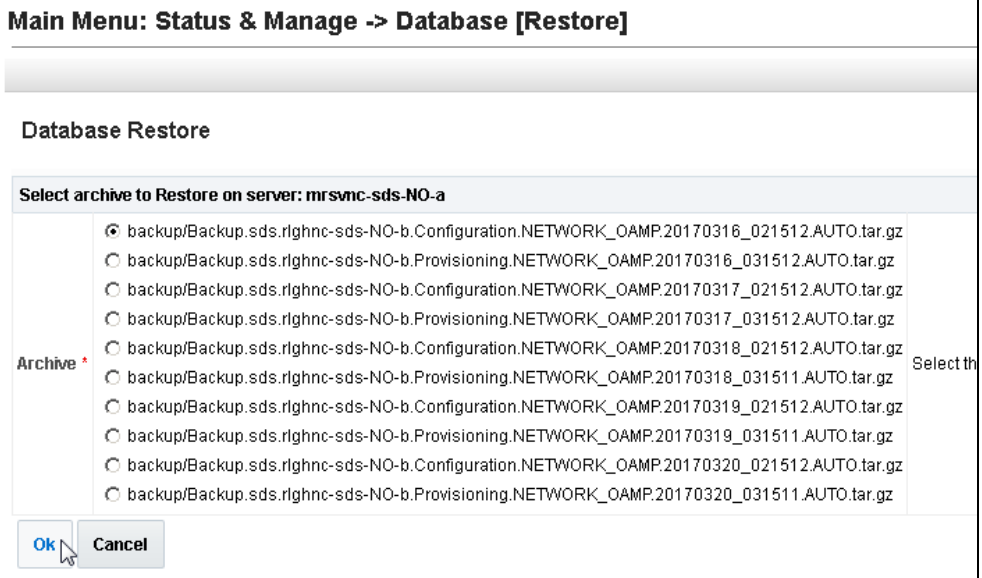
   Then you will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are one of Oracle’s Tekelec Customers new to MOS.

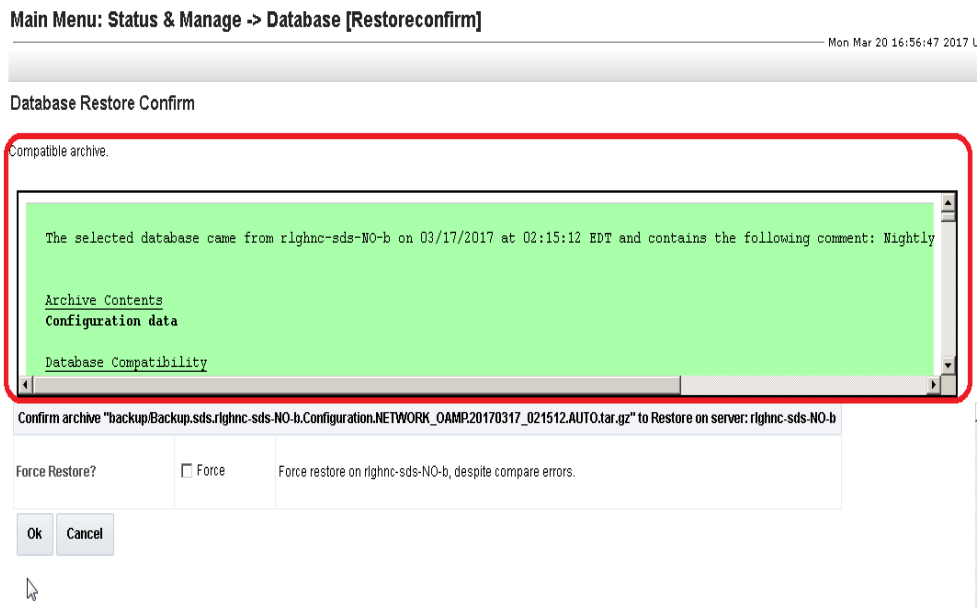
APPENDIX B: INSTALL NETBACKUP CLIENT

STEP #	Procedure	Description
1. ☐	Install Netbackup Client Software	Execute *Section 3.10.5 Application NetBackup Client Install/Upgrade Procedures* of reference [3] to complete this step. **NOTE**: Location of the bpstart_notify and bpend_notify scripts is required for the execution of this step. These scripts are located as follows: **/usr/TKLC/appworks/sbin/bpstart_notify** **/usr/TKLC/appworks/sbin/bpend_notify** **NOTE**: Netbackup client software must be installed on each SDS NOAM Server
2. ☐	Link notify scripts to well-known path stated in the above step	Link the notify scripts to well-known path stated in the above step **ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify** **ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify**
3. ☐	Verify if the Netbackup port 1556 is opened for IPv4 protocol	Verify if the NetBackup port 1556 is opened on IPv4 protocol: **iptables -L 60sds-INPUT -n | grep 1556** If there is no output, then enable the port 1556 for NetBackup on IPv4: **iptablesAdm append --type=rule --protocol=ipv4 --domain=60sds --table=filter --chain=INPUT --match='-m state --state NEW -m tcp -p tcp --dport 1556 -j ACCEPT' --persist=yes**
4. ☐	Verify if the Netbackup port 1556 is opened for IPv6 protocol	Verify if the NetBackup port 1556 is opened on IPv6 protocol: **ip6tables -L 60sds -INPUT -n | grep 1556** If there is no output, then enable the port 1556 for NetBackup on IPv6 protocol: **iptablesAdm append --type=rule --protocol=ipv6 --domain=60sds --table=filter --chain=INPUT --match='-m state --state NEW -m tcp -p tcp --dport 1556 -j ACCEPT' --persist=yes**
THIS PROCEDURE HAS BEEN COMPLETED		

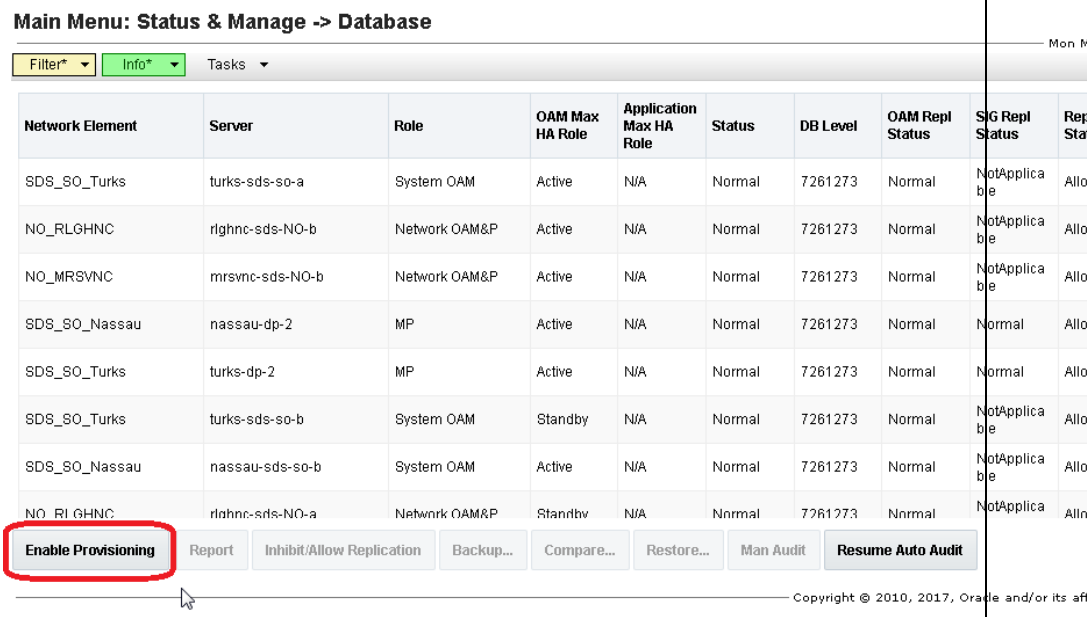
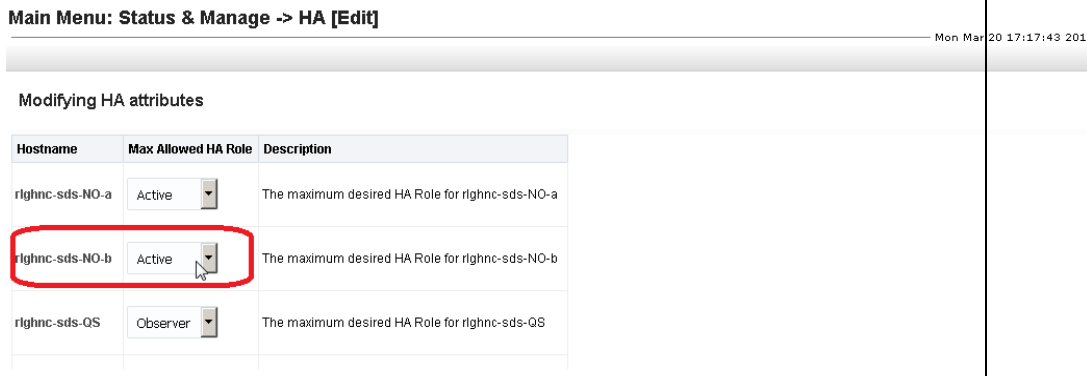
APPENDIX C: RESTORE PROVISIONING DATABASE

STEP #	Procedure	Description
1. ☐	Log into Primary SDS NOAM GUI	Log into Primary SDS NOAM GUI using its static IP (not the VIP).
2. ☐	Place the newly recovered Standby NOAM into Forced Standby	1. Navigate to **Main Menu: Status & Manage-> HA** 2. Click on **"Edit"** 3. Move the newly recovered standby server to forced standby. 

3. ☐	Restore Provisioning data	1. Navigate to **Main Menu: Status & Manage -> Database** 2. Select Select Active NOAM and click the Restore button.  3. Select Provisioning backup file from the list (which was previously placed in /var/TKLC/db/filemgmt/backup directory in Step 5 of Section 2.6.2) and click the OK button. **Note: Must use a Provisioning only backup file. Combined backup files containing Configuration & Provisioning data will cause catastrophic issues which could lead to complete re-installation.** 

STEP #	Procedure	Description
		4. Verify Compatibility and select Ok to restore. 
4. ☐	Wait for the restore to begin	Wait 60 seconds for the restore to begin.
5. ☐	Track Progress of Restore	Monitor the "Info" tab under the **[Status & Manage --> Database]** screen and look for the following message: **NOTE**: - Restore on <Active_NO_hostname> status MAINT_IN_PROGRESS.
6. ☐	Wait for the restore to complete	Continue to monitor the "Info" tab under the **[Status & Manage --> Database]** screen until the following message is received: Success: - Restore on rlghnc-sds-NO-b status MAINT_CMD_SUCCESS. Success NOTE: The “Info" tab may require manual refresh to see updated status. To refresh the "Info" tab, re-select **[Status & Manage --> Database]** from the Main Menu, then reselect the "Info" tab.

STEP #	Procedure	Description
7. ☐	Uninhibit servers	Uninhibit All servers in the following staggered arrangement: 1. Uninhibit Active NOAM. 2. Refresh/monitor the [Status & Manage --> Database] screen until a valid "DB Level" appears for the Active NOAM. 3. Uninhibit Standby NOAM / Query Server. 4. Refresh/monitor the [Status & Manage --> Database] screen until a valid "DB Level" appears for the Standby NOAM / Query Server. 5. Uninhibit Active SOAMs. 6. Refresh/monitor the [Status & Manage --> Database] screen until a valid "DB Level" appears for the Active SOAMs. 7. Uninhibit Standby SOAMs / DPs. 8. Refresh/monitor the [Status & Manage --> Database] screen until a valid "DB Level" appears for the Standby SOAMs / DPs.
8. ☐	Recover Pdbrelay (IF NEEDED)	Verify whether PDB Relay is Enabled by following the instructions in **Appendix D**.

STEP #	Procedure	Description
9. ☐	Enable Provisioning	Navigate to: [Status & Manage --> Database] and click “Enable Provisioning” 
10. ☐	Remove NO from forced standby.	1. Navigate to **Main Menu: Status & Manage -> HA** , click Edit. 2. Select the server which was moved to forced standby in **step 2**, change Max HA Role to Active and click OK. 
THIS PROCEDURE HAS BEEN COMPLETED		

APPENDIX D: RECOVER PDBRELAY

If, system fails to re-establish pdbrelay connection, follow the instructions:

STEP #	Procedure	Description
1. ☐	Determine if pdbrelay is enabled	Execute following command on console of Active NOAM server (accessed via the VIP) and compare the output: **$ iqt -zhp -fvalue ProvOptions where "var='pdbRelayEnabled'"** **TRUE** **$** **Proceed to next step only if the result of above command is true.**
2. ☐	Disable pdbrelay	Uncheck PDB Relay Enabled checkbox under the **[SDS --> Configuration --> Options]** screen and Apply the change.
3. ☐	Emergency Restart (Start from Beginning of Cmd Log)	Execute following commad on console: **$ iset -fvalue=0 ProvOptions where "var='pdbRelayMsgLogTimeStamp'"**
4. ☐	Enable pdbrelay	Recheck PDB Relay Enabled checkbox under the **[SDS --> Configuration --> Options]** screen and Apply the change.
THIS PROCEDURE HAS BEEN COMPLETED		

APPENDIX E: BACKUP DIRECTORY

This workaround helps to create backup directory with correct permissions if required.

STEP #	Procedure	Description
1 ☐	**NOAM/SOAM VIP console**: Determine if backup directory is created	Execute following command on console of Active NOAM/SOAM server (accessed via the VIP) and compare the output: **$ cd /var/TKLC/db/filemgmt/** **$ ls -ltr** Look for backup directory in the output. Check if directory is already created with correct permission. Directory will look like:- drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup In case, directory is already there with right permissions then skip steps 2 and 3. If directory is not with right permissions then execute step 3. Otherwise go to next step.
2 ☐	**NOAM/SOAM VIP console:** Create backup directory	Assuming present working directory is **/var/TKLC/db/filemgmt/** Otherwise, do **cd /var/TKLC/db/filemgmt/** #Create backup directory $mkdir backup **Verify directory is created:-** **$ ls -ltr /var/TKLC/db/filemgmt/backup** Error should not come "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content.
3 ☐	**NOAM/SOAM VIP console:** Change permissions of backup directory	Assuming backup directory is created **Verify directory is created:-** **$ ls -ltr /var/TKLC/db/filemgmt/backup** Error should not come "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content. If directory is not created go to step 2. Else proceed. #Change permissions of backup directory **$ chmod 770 /var/TKLC/db/filemgmt/backup** #Change ownership of backup directory **$ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup** After changing the permissions and ownership of the backup directory. **Directory will look like** **drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15 backup**

4 ☐	**NOAM/SOAM VIP console:** Copy the backup file which we need to restore in backup directory	Copy the backup file to backup directory $ **cp BACKUPFILE /var/TKLC/db/filemgmt/backup** Provide permissions to backup file inside backup directory. # Make sure about present working directory. $cd **/var/TKLC/db/filemgmt/backup** #Change permissions of files inside backup directory $chmod 666 Backup.* # Change ownership of files inside backup directory $ **sudo chown -R awadmin:awadm** Backup.*