Oracle® Communications

Diameter Signaling Router

SDS Disaster Recovery User's Guide

Release 8.3

E93226-01

September 2018

ORACLE®

Oracle Communications Diameter Signaling Router SDS Disaster Recovery User's Guide, Release 8.3

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 My Oracle Support (MOS) in Appendix E.

Table of Contents

List of Tables

List of Figures

List of Procedures

E93226-01

1. Introduction

This document describes procedures to use during disaster scenarios related to SDS 8.3 product.

The disaster scenarios covered in this 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.

1.1 References

[1] SDS Initial Installation Guide

[2] TPD Initial Product Manufacture, Software Installation Procedure

[3] 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

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Meaning
DP	Database Processor
DR	Disaster Recovery
MP	Message Processor
NOAM	Network Operations, Administration & Maintenance
OAM	Operations, Administration & Maintenance
SDS	Subscriber Data Server
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution (Linux OS)

Acronym	Meaning
VIP	Virtual IP
XMI	External Management Interface

1.3 Terminology

This section describes terminology as it is used within this document.

Table 2. Terminology

Term	Meaning
Upgrade	The process of converting an application from its current release on a system to a newer release.
Major upgrade	An upgrade from a current major release to a newer major release. An example of a major upgrade is SDS 7.3 to SDS 8.3.
Incremental upgrade	An upgrade from a current build to a newer build within the same major release. An example of an incremental upgrade is SDS 8.3.0.0.0_83.3.0 to 8.3.0.0.0_83.4.0.
Software only upgrade	An upgrade that does not require a database schema change; only the software is changed.
Single server upgrade	The process of converting an SDS server from its current release on a single server to a newer release.
Backout	The process of reverting a single SDS server to a prior version. This could be performed due to failure in single server upgrade.

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 the procedures in this document, there are a few key points to help ensure you understand procedure convention. These points are:

1. Before beginning a procedure, completely read the instructional text (it displays 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.

3. If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact My Oracle Support (MOS) for assistance, as described in Appendix E before attempting to continue.

Figure 1 shows an example of a procedural step used in this document.

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 and step 2 and substep 2.1.

- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.

- GUI fields and values to take note of during a step are in bold Arial font.

Each step has a checkbox the user should check to keep track of the progress of the procedure.

The Title column describes the operations to perform during that step.

Each command the user enters, and any response output, is formatted in 10-point Courier font.

	Title/Instructions	Directive/Result Steps
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	Verify Network Element data	1. View the Network Elements configuration data; verify the data; save and print report. 2. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example Procedure Steps Used in This Document

2. Disaster Recovery Scenarios

 !!WARNING!!

Whenever there is need to restore the database backup for NOAM and SOAM servers in any of the below recovery scenarios, the backup directory may not be there in the system since system is in DRed.

In this case, refer to Appendix D Backup Directory to 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

To make SDS GUI accessible and continue provisioning, follow these instructions:

1. To promote the DR NOAM from secondary to primary, follow reference [6].
2. To recover primary NOAM as DRNO, follow reference [6].

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 the 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 Replace 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

Procedure 1. Replace a DP Server		
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 the VIP address, log into the SOAM GUI site where the defective DP server is located. 2. Navigate to **Status and Manage > Server**. 3. Select the defective DP server by its hostname. 4. Click **Stop**. 5. Click **OK** on confirmation screen.
3. ☐	Verify no signaling traffic is processed at the defective DP server	1. Navigate to **Status and Manage > KPIs**. 2. Click the KPI filter icon on the right side of the screen. 3. Click **DP** for Group. 4. Click **GO**. 5. Select the tab for the DP server to recover. 6. Verify the **Total Queries/Sec** KPI is now showing **0** for this DP.

4. ☐	Power down the defective DP server	*Note:* If HW replacement is deemed necessary, physically remove the defective DP blade and install the new replacement blade.
		
		 1. Power down the defective DP server.
		
		 2. Label all cables connected to defective DP server.
		
		 3. Physically remove the defective DP server from the frame.
		
		 4. To install the new DP blade, use these steps from reference [7]:
		     a. Upgrade firmware on the Blade.
		     b. Upgrade the BIOS of the Blade.
		     c. Set the iLO credentials userid/password of the Blade.
		
		 5. Power up the new DP server.

Procedure 1.	Replace a DP Server	
5. ☐	Install the 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 through 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 reference [1].
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. Navigate to **Status and Manage > KPIs**. 2. Click the KPI filter icon on the right side of the screen. 3. Click **DP** for Group. 4. Click **GO**. 5. Select the tab for the DP server to recover. 6. Verify the **Total Queries/Sec** KPI is now showing a non-zero value for this DP.
10. ☐	Verify ComAgent connections	1. Navigate to **Communication Agent > Maintenance > Connection Status**. 2. Verify ComAgent connections (Automatic and Configured).

2.2.3   Post-Condition

DP server is processing traffic.

2.3 Replace 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

Procedure 2.	Replace a SOAM Server	
1. ☐	Prepare for server replacement	Identify the SOAM server that needs to be replaced. Defective SOAM server hostname = _____

Procedure 2.		Replace a SOAM Server
2. ☐	Make SOAM server's Max Allowed HA Role **Standby** so it does not become active	1. Log into the primary SDS NOAM GUI as the **admin** user using the VIP address. 2. Navigate to **Status and Manage > HA**. 3. Click **Edit**. 4. Change the **Max Allowed HA Role** of the defective SOAM server to **Standby**. 5. Click **OK**.
3. ☐	Remove SOAM server from the server group	1. Navigate to **Configuration > Server Groups**. 2. Select SOAM's server group. 3. Click **Edit**. 4. Under **SG Inclusion**, uncheck the defective SOAM server. 5. Click **OK**.
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. ☐	Install SDS application on the new SOAM server	Execute procedure 8, steps 1 through 22 (Installing the SDS Application) from reference [1].
6. ☐	Prepare the new SOAM server	Execute procedure 8, steps 45 through 74 (Applying TKLCConfigData.sh File on the New SOAM Server) from reference [1].
7. ☐	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].
8. ☐	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 Replace 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

Procedure 3.		Replace a Query Server
1. ☐	Prepare for Query server replacement	Identify the defective Query server that needs to be replaced. Defective Query server hostname = _____

Procedure 3.	Replace a Query Server	
2. ☐	Remove the defective Query Server from the server group	1. From the SDS GUI, navigate to **Configuration > Server Groups**. 2. Select Query server's server group. 3. Click **Edit**. 4. Under **SG Inclusion**, uncheck the defective Query server. 5. Click **OK**.

3. ☐	Power down and replace Query server	Power down the defective Query server.
		Label all cables connected to the defective Query server.
		Physically remove the defective Query server from the frame
		All connections should be made to the replacement server according to the labels attached in **sub-step 2** of the same step
		Power up the new Query server
		 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 Replace 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

Procedure 4.	Replace a SDS NOAM Server	
1. ☐	Prepare for server replacement	Identify the defective SDS NOAM server that needs to be replaced. Defective SDS NOAM server hostname = _____

Procedure 4.	Replace a SDS NOAM Server	
2. ☐	Make the defective SDS NOAM server's Max Allowed HA Role **Standby** so it does not become active	1. Log into the primary SDS GUI as the **admin** user using the VIP address. 2. Navigate to **Status and Manage > HA**. 3. Click **Edit**. 4. Change the **Max Allowed HA Role** of the defective SDS NOAM server to **Standby**. 5. Click **OK**.
3. ☐	Remove the SDS NOAM server from the server group	1. Navigate to **Configuration > Server Groups**. 2. Select SDS's server group. 3. Click **Edit**. 4. Under **SG Inclusion**, uncheck the defective SDS NOAM server. 5. Click **OK**.

4. ☐	Power down and replace the 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. Make all connections to the replacement server according to the labels attached in **sub-step 2** of this same step.
		
		5. Power up the new SDS NOAM server.
		
		6. To install the new NOAM server, use these step from reference [7]:
		
		   a. Check/upgrade firmware on the Blade
		
		   b. Upgrade the BIOS of the Blade.
		
		   c. 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 the SDS NOAM server	Execute procedure 2, steps 26 through 49 , then Steps 52 through 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].
8. ☐	Restart the application on new SDS NOAM server	Execute procedure 3, steps 26 through 40 (Pairing the SDS NOAM Servers) from reference [1].

Procedure 4.		Replace a SDS NOAM Server
9. ☐	Re-exchange SSH keys for Remote Import, Remote Export, and Data Export features	1. Log into the primary SDS GUI as the **admin** user using the VIP address. 2. Perform SSH key exchange for Remote Export by navigating to **SDS** > **Configuration** > **Options**. 3. Perform SSH key exchange for Remote Import by navigating to **SDS** > **Configuration** > **Options**. 4. Perform SSH key exchange for Data Export by navigating to **Administration** > **Remote Servers** > **Data Export**.
10. ☐	Install NetBackup client software (optional)	Execute steps as described in Appendix A.

2.5.3   Post-Condition

SDS NOAM server is back in service.

2.6 Replace a 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

Procedure 5.	Replace a Primary SDS NOAM Server Pair	

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 _____
		Note: The backup archive files should be in uncompressed format.
		
		If it is not uncompress, then execute these commands:
		For gunzip file:
		
		```\n$ gunzip Backup.sds.sds1-noa-\n1191038.Configuration.NETWORK_OAMP.20160609_0215\n11.AUTO.tar.gz\n$ gunzip Backup.sds.sds1-noa-1191038.\nProvisioning.NETWORK_OAMP.20160609_021511.AUTO.t\nar.gz\n```
		For bunzip file:
		
		```\n$ bunzip2 Backup.sds.sds1-noa-\n1191038.Configuration.NETWORK_OAMP.20160609_0215\n11.AUTO.tar.bz2\n$ bunzip2 Backup.sds.sds1-noa-1191038.\nProvisioning.NETWORK_OAMP.20160609_021511.AUTO.t\nar.bz2\n```

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 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 these steps from reference [7]:
		   a. Check/upgrade firmware on the Blade.
		   b. Upgrade the BIOS of the Blade.
		   c. 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 a temporary external IP address on the new primary SDS-A server as described in Appendix C from reference [1].

Procedure 5.	Replace a Primary SDS NOAM Server Pair	
5. ☐	Copy SDS backup archive files to the new primary SDS-A server	1. Login using ssh to the console of the new primary SDS-A server. 2. Execute these 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** on the newly installed primary SDS-A server. 4. Execute this command to stop running applications. Leave the 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> ``` SDS database is now restored. 6. 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].
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 B.

10. ☐	Install the SDS application on the new primary SDS Query server	1. To install the new Query server, use these steps from reference [1].
		
		   a. Check/upgrade firmware on the Blade.
		
		   b. Upgrade the BIOS of the Blade.
		
		   c. Set the ILO credentials userid/password of the Blade.
		
		2. Execute procedure 1 on the new primary SDS Query server (Installing the SDS Application) from reference [1].

Procedure 5.	Replace a Primary SDS NOAM Server Pair	
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. Log into the primary SDS GUI as the **admin** user using the VIP address. 2. Navigate to **Status and Manage > Server**. 3. Select the primary SDS-A server. 4. Click **Restart**. 5. Click **OK** to confirm. 6. Repeat for the 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 A.
14. ☐	Re-exchange SSH keys for Remote Import, Remote Export, and Data Export features	1. Log into the primary SDS GUI as the **admin** user using the VIP address. 2. Perform SSH key exchange for Remote Export by navigating to **SDS** > **Configuration** > **Options**. 3. Perform SSH key exchange for Remote Import by navigating to **SDS** > **Configuration** > **Options**. 4. Perform SSH key exchange for Data Export by navigating to **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 Replace a 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

Procedure 6. Replace a SOAM Server Pair		
1. ☐	Prepare for server replacement	Identify the SOAM-A and SOAM-B servers that need to be replaced. 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 has a DB Level of **UNKNOWN** until the SOAMs are restored.	1. Log into the NOAMP GUI. 2. Navigate to **Status and Manage > Database**. 3. Filter on the SOAM Network Element name. 4. Record the DP server hostnames (Role: MP). 5. Click **Inhibit Replication** for each DP server until all DP servers associated with this SOAM Network Element have been inhibited. 6. Click **Inhibit Replication** for each defective SOAM server identified in sub-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. Log into the NOAMP GUI. 2. Navigate to **Status and Manage > Database**. 3. Filter on the SOAM Network Element name. 4. Record the DP server hostnames (Role: MP). 5. Click **Allow Replication** for each newly replaced SOAM-A and SOAM-B server. 6. Click **Allow Replication** 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].

Procedure 6. Replace a SOAM Server Pair		
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. Log into active SOAM GUI using the VIP address. 2. Navigate to **Status and Manage > Servers**. 3. Make sure the new SOAM servers show **Norm** for DB, Reporting Status, and Appl State.
12. ☐	Verify that SOAM servers showng valid DB level	1. Log into active SOAM GUI using the VIP address. 2. Navigate to **Status and Manage > Servers**. 3. Verify 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 Replace a 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

Procedure 7. Replace a DR SDS NOAM Server Pair		
1. ☐	Prepare for server replacement	Identify the DR SDS NOAM servers that need to be replaced. DR SDS-A server _____ DR SDS-B server _____ DR SDS Query server _____

Procedure 7.	Replace a DR SDS NOAM Server Pair	

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 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 these steps from reference [1]:
		   a. Check/upgrade firmware on the Blade.
		   b. Upgrade the BIOS of the Blade.
		   c. 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	1. Execute procedure 5, steps 22 through 45 on the new DR SDS-A server (Applying TKLCConfigData.sh File) from reference [1]. 2. 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	1. Execute procedure 5, steps 22 through 45 on the new DR SDS-B server (Applying TKLCConfigData.sh File) from reference [1]. 2. 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	1. Execute procedure 4, steps 17 through 43 on the new Query server (Applying TKLCConfigData.sh File) from reference [1]. 2. Execute procedure 4 (Configuring the Query Server), steps 54 through 56 (Restarting Application on DR SDS Query Server) from reference [1].
9. ☐	Verify DB level	Navigate to **Status and Manage > Database** and verify a valid DB Level 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 A.

Procedure 7.	Replace a DR SDS NOAM Server Pair	
11. ☐	Re-exchange SSH keys for Remote Import, Remote Export, and Data Export features	1. Log into the primary SDS GUI as the **admin** user using the VIP address. 2. Perform SSH key exchange for Remote Export by navigating to **SDS** > **Configuration** > **Options**. 3. Perform SSH key exchange for Remote Import by navigating to **SDS** > **Configuration** > **Options**. 4. Perform SSH key exchange for Data Export by navigating to **Administration** > **Remote Servers** > **Data Export**.

2.8.3 Post-Condition

All DR SDS NOAM servers are back in service.

2.9 Replace a SDS Frame

2.9.1 Pre-Condition

- SDS frame is destroyed.
- A replacement SDS frame with two SDS NOAM servers and a Query server are available.
- DR SDS NOAM servers are available.
- Access to DR SDS GUI is functional.

2.9.2 Recovery Steps

Procedure 8.	Replace a SDS Frame	
1. ☐	Determine SDS site and status of provisioning	If the destroyed SDS frame was the primary SDS frame, then execute the procedure from reference [6] to activate the 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 the new DR SDS NOAM servers into the new DR SDS frame by following instructions in reference [7].
4. ☐	Install switches in new DR SDS frame	Install new switches into the new DR SDS frame by following instructions in reference [7].
5. ☐	Connect DR SDS NOAM servers	Wire 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 Replace a 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

Procedure 9. Replace a SOAM Frame		
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 Blade System 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 Replace 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 for Cisco 4948E-F Switch1A for all SDS NOAM sites.

Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		
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 the 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 netConfig switch xml files exist on 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 My Oracle Support (MOS) for assistance.

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.
		Check the FW on the mate switch:
		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```

Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		
8. ☐	**Server A**: Verify the 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```

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.
		
		```$ 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.**

Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		

14. ☐	**Server A**: Get PROM information	*Note:* ROM and PROM are intended to have the same meaning for this procedure.
		
		 1. 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).
			
			 2. Note the IOS image and ROM version for comparison in a following step.
			
			 3. Exit from the console by pressing **<Ctrl-e><c><.>** and you are returned to the server prompt.
			
			 4. 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.

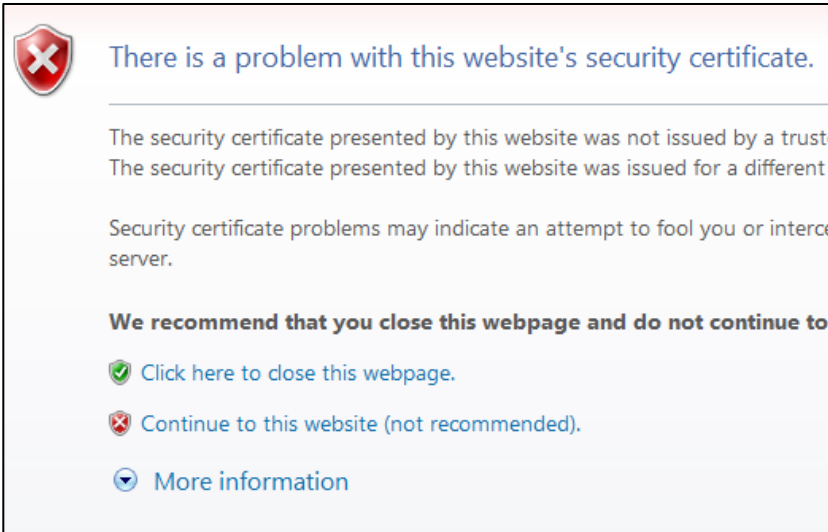| Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		
15. ☐	**Server A**: Reset switch to factory defaults	1. Connect serially to the switch and reload the switch by issuing the following commands. ```\nSwitch>en\nSwitch#write erase\nErasing the nvram filesystem will remove all\nconfiguration files! Continue? [confirm]\n[OK]\nErase of nvram: complete\n Switch#reload\n Proceed with reload? [confirm]\n```
		2. Wait until the switch reloads, then exit from console; press **<Ctrl-e><c><.>** and you are returned to the server prompt.
		3. Wait for the first switch to finish before repeating this process for the second switch.
		Note: There may be messages from the switch. If asked to confirm, press **Enter**. If asked yes or no, type **no** and press **Enter**.
16. ☐	**Server A**: Initialize switch	If replacing switch1A, issue this command: ```\nsudo netConfig --\nfile=/usr/TKLC/plat/etc/switch/xml/switch1A_SDS_4\n948E_E-F_init.xml\```
		If replacing switch1B, issue the following command: ```\nsudo netConfig --\nfile=/usr/TKLC/plat/etc/switch/xml/switch1B_SDS_4\n948E_E-F_init.xml\```
		Sample output from command: ```\nProcessing file:\n=/usr/TKLC/plat/etc/switch/xml/switch1A_SDS_4948E_E-\nF_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: ```\n$ sudo /usr/TKLC/plat/bin/netConfig --\ndevice=switch1A getHostname\nHostname: switch1A\```
		For switch1B: ```\n$ sudo /usr/TKLC/plat/bin/netConfig --\ndevice=switch1B getHostname\nHostname: 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).

Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		

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```
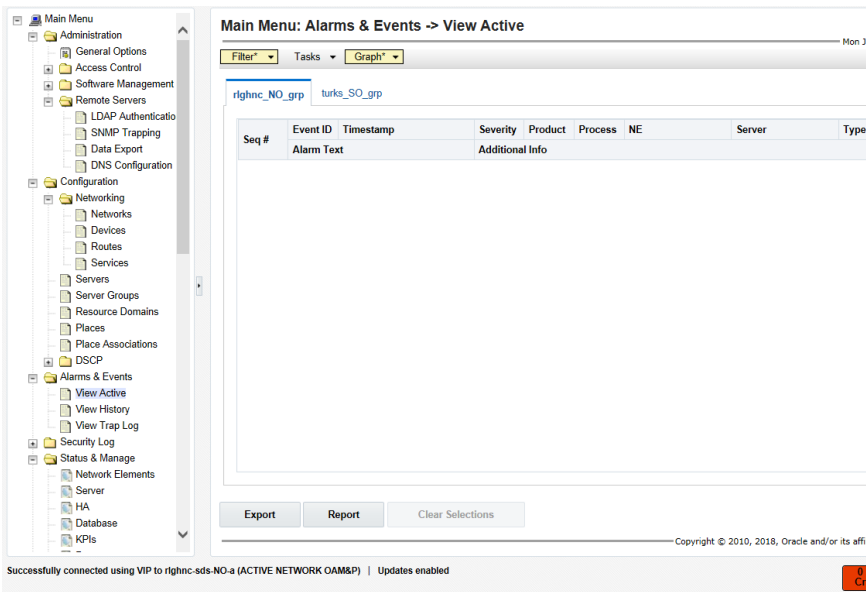		
		Note: The configuration of both switches should be very similar. As a guideline, the configuration of the recovered switch can be compared to the existing configuration of the mate switch.

Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		

18. ☐	**Server A**: Verify switch is using proper IOS image per firmware release notes	Verify the switch is using the proper IOS image:
		For switch1A:
		<pre>$ sudo /usr/TKLC/plat/bin/netConfig --
		device=switch1A getFirmware</pre>
		For switch1B:
		<pre>$ sudo /usr/TKLC/plat/bin/netConfig --
		device=switch1B getFirmware</pre><pre>Version: 122-54.WO
		License: entservicesk9
		Flash: cat4500e-entservicesk9-mz.122-54.WO.bin</pre>

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

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

21. ☐	**Server A**: Remove the iptables rule to allow TFTP	<pre>$ 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"</pre>

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

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. <pre>$ sudo /sbin/ifup <NIC to switch></pre> **If switch1A is being recovered, bring eth11 up** **If switch1B is being recovered, bring eth01 up.**

Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		
24. ☐	**Server A**: Ensure both interfaces of bond0 are up	Ensure the bond0 interfaces are both up. ```$ 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```
25. ☐	**Server A**: Verify ping to both switches	Ping each switch's SVI (router interface) addresses to verify switch configuration. ```$ /bin/ping 169.254.1.1` `$ /bin/ping 169.254.1.2```

Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		
26. ☐	**Primary SDS VIP**: Connect to active SDS site	From a web browser, connect to the XMI VIP address of the active SDS site. ***Note:*** If presented with the **security certificate** warning screen, select **Continue to this website (not recommended)**.
27. ☐	**Primary SDS VIP**: Login	Log into the GUI using the default user and password.

Procedure 10. Replace a Failed 4948/4948E/4948E-F Switch		
28. ☐	**SDS VIP**: Verify alarm status	1. Navigate to **Alarms and Events > View Active**. 2. Verify no alarms exist on the reporting device interface or replication issues.

2.11.3 Post-Condition

The switch 4948 is replaced and back in service.

Appendix A. Install NetBackup Client
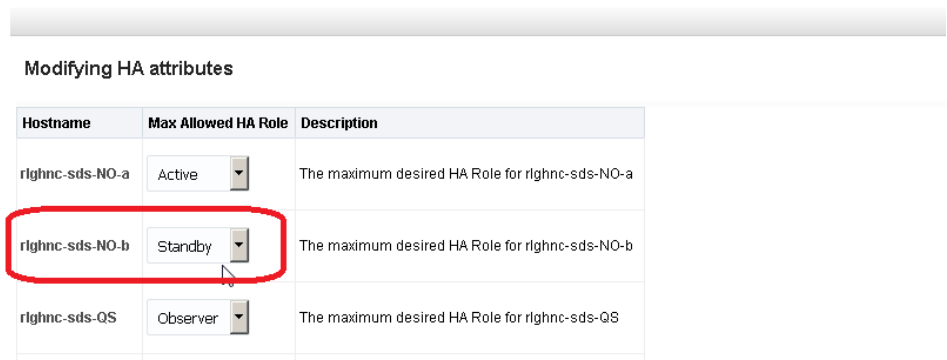
Procedure 11. Install NetBackup Client		

1. ☐	Install NetBackup client software	Execute Section 3.10.5 Application NetBackup Client Install/Upgrade Procedures in reference [3] to complete this step.
		Locate the **bpstart_notify** and **bpend_notify** scripts to execute this step. These scripts are located in:
		
		`/usr/TKLC/appworks/sbin/bpstart_notify`
		`/usr/TKLC/appworks/sbin/bpend_notify`
		
		The NetBackup client software must be installed on each SDS NOAM server.

2. ☐	Link notify scripts to known path stated in step 1	`ln -s <path>/bpstart_notify`
		`/usr/openv/netbackup/bin/bpstart_notify`
		`ln -s <path>/bpend_notify`
		`/usr/openv/netbackup/bin/bpend_notify`

3. ☐	Verify the NetBackup 1556 port is open for IPv4 protocol	`iptables –L 60sds-INPUT -n	grep 1556` If there is no output, then enable the 1556 port 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`

Procedure 11. Install NetBackup Client		

4. ☐	Verify the NetBackup 1556 port is open for IPv6 protocol	`ip6tables –L 60sds –INPUT –n | grep 1556`
		If there is no output, then enable the 1556 port for NetBackup on IPv6:
		<pre>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</pre>

Appendix B.   Restore Provisioning Database

This procedure restores the SDS provisioning database.

Procedure 12. Restore Provisiong Database		
1. ☐	**Primary SDS NOAM GUI**: Log into the primary SDS NOAM GUI	Log into primary SDS NOAM GUI using its static IP (not the VIP).
2. ☐	**Primary SDS NOAM GUI**: Place the newly recovered standby NOAM into forced standby	1. Navigate to **Status and Manage > HA**. 2. Click **Edit**. 3. Move the newly recovered standby server to forced **Standby**. **Main Menu: Status & Manage -> HA [Edit]** Modifying HA attributes | Hostname	Max Allowed HA Role	Description
rlghnc-sds-NO-a	Active	The maximum desired HA Role for rlghnc-sds-NO-a
rlghnc-sds-NO-b	Standby	The maximum desired HA Role for rlghnc-sds-NO-b
rlghnc-sds-QS	Observer	The maximum desired HA Role for rlghnc-sds-QS	
3. ☐	**Primary SDS NOAM GUI**: Restore provisioning data	1. Navigate to **Status and Manage > Database**. 2. Select the active NOAM and click **Restore**.

Procedure 12. Restore Provisiong Database

Main Menu: Status & Manage -> Database

3. Select the **Provisioning backup** file from the list (which was previously placed in the **/var/TKLC/db/filemgmt/backup** directory in step 5 of section 2.6.2) and click **OK**.

    Note: You must use a provisioning only backup file. Combined backup files contain configuration and provisioning data and cause catastrophic issues, which could lead to a complete re-installation.

Main Menu: Status & Manage -> Database [Restore]

Database Restore

Select archive to Restore on server: mrsvnc-sds-NO-a

Archive *	
	⊙ backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170316_021512.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170316_031512.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170317_021512.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170317_031512.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170318_021512.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170318_031511.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170319_021512.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170319_031511.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170320_021512.AUTO.tar.gz
	○ backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170320_031511.AUTO.tar.gz

Ok   Cancel

4. Verify compatibility and click **OK** to restore.

Procedure 12. Restore Provisiong Database		
		Main Menu: Status & Manage -> Database [Restoreconfirm] Mon Mar 20 16:56:47 2017 L Database Restore Confirm Compatible archive. The selected database came from rlghnc-sds-NO-b on 03/17/2017 at 02:15:12 EDT and contains the following comment: Nightly Archive Contents **Configuration data** Database Compatibility Confirm archive "backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170317_021512.AUTO.tar.gz" to Restore on server: rlghnc-sds-NO-b Force Restore? ☐ Force Force restore on rlghnc-sds-NO-b, despite compare errors. Ok Cancel
4. ☐	**Primary SDS NOAM GUI**: Wait for the restore to begin and track progress until the restore is complete	1. Wait 60 seconds for the restore to begin. 2. Monitor the Info tab under the **Status and Manage > Database** screen and look for the following message: Restore on <Active_NO_hostname> status MAINT_IN_PROGRESS. 3. Wait for the restore to complete by looking for the following message: Success: - Restore on rlghnc-sds-NO-b status MAINT_CMD_SUCCESS. Success *Note:* Refresh the Info tab manually to see updated status by navigating to Status and Manage > Database again and selecting the Info tab.
5. ☐	Primary SDS NOAM GUI: Uninhibit servers	Uninhibit all servers in the following staggered arrangement: 1. Uninhibit active NOAM. Refresh/monitor the **Status and Manage > Database** screen until a valid **DB Level** displays for the active NOAM. 2. Uninhibit **standby** NOAM/Query server. Refresh/monitor the **Status and Manage > Database** screen until a valid **DB Level** displays for the standby NOAM/Query server. 3. Uninhibit **active** SOAMs. Refresh/monitor the **Status and Manage > Database** screen until a valid **DB Level** displays for the active SOAMs. 4. Uninhibit **standby** SOAMs/DPs. Refresh/monitor the **Status and Manage > Database** screen until a valid **DB Level** displays for the standby SOAMs/DPs.
6. ☐	Recover Pdbrelay (if needed)	Verify whether PDB Relay is **Enabled** by following the instructions in Appendix C Recover PDB Relay.

Procedure 12. Restore Provisiong Database		
7. ☐	**Primary SDS NOAM GUI**: Enable provisioning	Navigate to **Status and Manage > Database** and click **Enable Provisioning**.
8. ☐	**Primary SDS NOAM GUI**: Remove NO from forced standby	1. Navigate to **Status and Manage > HA** and click **Edit**. 2. Select the server, which was moved to forced standby in step 2, change **Max HA Role** to **Active**, and click **OK**.

Appendix C.   Recover PDB Relay

If the system fails to re-establish a PDB relay connection, follow this procedure.

Procedure 13. Recover PDB Relay		

1.
☐
	NOAM VIP console: 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. ☐	**NOAM VIP GUI**: Disable pdbrelay	Unmark the **PDB Relay Enabled** checkbox on the **SDS > Configuration > Options** screen and click **Apply**.

Procedure 13.	Recover PDB Relay	

3. ☐	**NOAM VIP Console**: Emergency restart (start from beginning of Cmd log)	Execute following command on console:
		
		``
		$ iset -fvalue=0 ProvOptions where
		"var='pdbRelayMsgLogTimeStamp'"
		``

4. ☐	**NOAM VIP GUI**: Enable pdbrelay	Mark the **PDB Relay Enabled** checkbox on the **SDS > Configuration > Options** screen and click **Apply**.

Appendix D.   Backup Directory

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

Procedure 14.	Backup Directory	

1. ☐	**NOAM/SOAM VIP Console**: Determine if backup directory exists	1. Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output.
		
		``
		$ cd /var/TKLC/db/filemgmt/
		$ ls -ltr
		``
		
		2. Look for the backup directory in the output.
		
		3. Make sure the directory is already created with correct permission. The directory looks like this:
		
		``
		drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup
		``
		
		4. If the directory is already there with correct permissions, then skip steps 2 and 3.
		
		5. If directory does not have the correct permissions, then go to step 3.

2. ☐	**NOAM/SOAM VIP Console**: Create backup directory	1. Go to the backup directory location.
		
		``
		cd /var/TKLC/db/filemgmt/
		``
		
		2. Create backup directory.
		
		``
		$ mkdir backup
		``
		
		3. Verify directory has been created.
		
		``
		$ ls -ltr /var/TKLC/db/filemgmt/backup
		``
		
		Note: A **No such file or directory** error message should not display. The directory should show as empty with the total as 0 for content.

Procedure 14. Backup Directory		

3. ☐	**NOAM/SOAM VIP Console**: Change permissions of backup directory	1. Verify directory has been created.
		
		`$ ls -ltr /var/TKLC/db/filemgmt/backup`
		
		Note: A **No such file or directory** error message should not display. The directory should show as empty with the total as 0 for content.
		
		2. Change permissions for the backup directory.
		
		`$ chmod 770 /var/TKLC/db/filemgmt/backup`
		
		3. Change ownership of backup directory.
		
		`$ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup`
		
		4. Directory displays as follows:
		
		`drwxrwx--- 2 awadmin awadm      4096 Dec 22 02:15 backup`

4. ☐	**NOAM/SOAM VIP Console**: Copy the backup file to the backup directory	1. Copy the backup file to the backup directory.
		
		`$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup`
		
		2. Change permissions of files in the backup directory.
		
		`$ chmod 666 Backup.*`
		
		3. Change ownership of files in the backup directory.
		
		`$ sudo chown -R awadmin:awadm Backup.*`

Appendix E.   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 US), 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, make the selections in the sequence shown on the Support telephone menu:

1. Select **2** for New Service Request.

2. Select **3** for Hardware, Networking and Solaris Operating System Support.

3. Select one of the following options:

    For technical issues such as creating a new Service Request (SR), select 1.

    For non-technical issues such as registration or assistance with MOS, select 2.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability

- Significant reduction in system capacity or traffic handling capability

- Loss of the system's ability to perform automatic system reconfiguration

- Inability to restart a processor or the system

- Corruption of system databases that requires service affecting corrective actions

- Loss of access for maintenance or recovery operations

- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the **Oracle Help Center** site at http://docs.oracle.com.

2. Click Industries.

3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure or Platforms.

4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays.

5. To download a file to your location, right-click the PDF link, select **Save target as** (or similar command based on your browser), and save to a local folder.