Oracle® Communications
Diameter Signaling Router Full Address Resolution

SDS Disaster Recovery User's Guide

Release 7.1

E59145, Revision 02

August 2015

ORACLE®

Oracle® Communications Diameter Signaling Router Full Address Resolution, SDS Disaster Recovery, Release 7.1

Copyright © 2011, 2015

Oracle and/or its affiliates. All rights reserved.

TABLE OF CONTENTS

List of Tables

1.0   INTRODUCTION

1.1   Purpose and Scope

This document describes procedures to use during disaster scenarios related to SDS 7.1 product.

The disaster scenarios covered in document are:

1. Connectivity loss to Primary SDS 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 server

6. A defective SDS 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 Oracle's Tekelec Customer Service team on fielded SDS systems.

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

1.2   References

External *(Customer Facing):*

[1] SDS 7.1 Initial Installation Guide, E58856
[2] TPD Initial Product Manufacture, Software Installation Procedure, Release 7.0+, E53017
[3] Platform 7.0 Configuration Guide, E53486
[4] DSR 5.x/6.x/7.0 3-Tier Disaster Recovery Guide, E57520-01
[5] Cabinet Assembly Instructions, 910-6083-001

Internal *(Available to Oracle's Tekelec personnel only):*

[6] ALEXA 5.0 HP c-Class & Rack-mount Server Site Installation and Configuration, TR007011
[7] Network Interconnect. Topology 1 with Variants. TR007111
[8] Platform 5.0 Generic HP c-Class Networking Interconnect, TR006851
[9] DSR Network Planning for AT&T Mobility – LTE, MS006641
[10] BL460cc Hardware Upgrade AT&T PAS Lab, WI006803
[11] SDS 7.1 Software Upgrade Guide, E60672

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	Network Operations, Administration & Maintenance
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

2.1   Complete connectivity loss of Primary SDS 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, old-DR SDS servers are activated and made to serve as new-Primary SDS servers via the following steps:

1 ☐	Disable the application on DR SDS servers.	This step ensures that when the DR SDS assumes new-Primary SDS status in a controlled fashion. Disabling the application inhibits provisioning and can be started after successful validation. 1. Using VIP address, login to the DR SDS GUI as admin user. 2. Navigate to GUI screen [**Main Menu: Status & Manage → Server**] 3. Select the row that has active DR SDS server. It highlights 'Stop' button at the bottom. 4. Click the 'Stop' button and then click the 'OK' button. At this time, HA switch over causes an automatic logout. 5. Repeat step all above sub-steps for new active DR SDS server. 6. Verify that 'Proc' column on both DR SDS servers show 'Man' indicating that application is manually stopped.
2 ☐	SSH to VIP address of the DR SDS as root and make it primary SDS	1. Using VIP address, login to DR SDS Active server console. 2. Execute the command to take DR SDS site over as the new-Primary SDS site `# top.setPrimary` 3. System generates several replication and collection alarms as replication/collection links to/from former Primary SDS servers becomes inactive.
3 ☐	Clear any persistent alarms	1. Wait at least 5 minutes for replication to rsync ("inetmerge" or "inetrep" alarms may remain present). 2. If inetmerge or inetrep alarms persist beyond 5 minutes, then on the new primary SDS, restart the corresponding process(es): `# pm.kill  <inetmerge or inetrep>` 3. View alarms until all is cleared.
4 ☐	Verify the replication	1. Navigate to GUI screen [**Main Menu: Status & Manage → Server**] at new-Primary SDS, and monitor replication status. 2. It may take several minutes for DB replication to complete, afterwards "DB" and "Reporting Status" columns should show 'Normal.'

5 ☐	Re-enable the application on the now-Primary SDS using the Active new-Primary SDS GUI.	1. Using VIP address, login to new-Primary SDS GUI as admin user. 2. Navigate to GUI screen [**Main Menu: Status & Manage → Server**] 3. Select the row that has the new-Primary SDS Active server. This will highlight the 'Restart' button at the bottom. 4. Click the 'Restart' button and then click the 'OK' button. 5. Verify that 'Proc' column now shows 'Norm'. 6. Repeat sub-steps 3 to 5 for new-Primary SDS Standby server.

6 ☐	Decrease the durability admin status and then reconfigure and reconnect the customer's provisioning clients.	1. Lower the durability admin status to 2 (NO pair) to exclude former-Primary SDS servers from the provisioning database durability. A value greater than 2 must be adjusted downward.
		
		  a. Using VIP address, login to new-Primary SDS GUI as admin user
		
		  b. Navigate to GUI screen [**Main Menu: Administration → General Options**]
		
		  c. Set *durableAdminState* to 2 (NO pair)
		
		  d. Click the 'OK' button
		
		2. Provisioning connections can now resume to the VIP of the new-Primary SDS. Have customer reconfigure provisioning clients to connect to XMI VIP of the newly activated Primary SDS servers.
		
		3. Verify that DB provisioning from clients has started.
		
		  a. Select [**Main Menu: SDS → Maintenance → Command Log**]
		
		  b. Check that new DB provisioning commands have been executed

	At this point, SDS provisioning is fully functioning. The remaining steps will bring the former-Primary SDS servers back into the service as the new-DR SDS servers.	

7 ☐	Bring former-Primary SDS back to service.	1. Determine what has happened to former-Primary SDS site.
		
		  • SDS frame defective ?_____
		  • SDS servers defective ? _____
		  • Networking outage ? _____
		  • Switch defective ? _____
		
		2. Based on the above disaster recovery scenario, execute procedure from this document to return the former-Primary SDS servers and site back to service.

8 ☐	Convert former Primary SDS servers to new DR SDS	1. SSH to active former-Primary SDS server as root. 2. Execute the command to take formerly Primary SDS as the DR SDS site `# top.setSecondary` 3. Monitor [**Main Menu: Status & Manage → Server**] screen at new DR SDS GUI. 4. It may take several minutes for replication, afterward the DB and Reporting Status columns should show 'Normal.'

9 ☐	Stop Non-Service processes on DR	1. Select [**Main Menu: Status & Manage → Server**] for now Active DR SDS on GUI.
		2. Press the 'Stop' button for new DR SDS (stops *all* processes).
		3. Press the 'OK' button to confirm.
		4. Again select [**Main Menu: Status & Manage → Server**] for new DR SDS on GUI.
		5. Press the 'Restart' button for new DR SDS (starts *only* Service processes).
		6. Press the 'OK' button to confirm.
		7. Monitor [**Main Menu: Status & Manage → Server**] screen for new DR SDS on GUI.
		8. It may take a few seconds, but afterward the Application State should be 'Enabled,' and the Alarm and Process Status columns should show 'Normal.'
10 ☐	Set durability admin status to include DR SDS servers back to the replication	1. If you reduced the durability status in step 6, then raise durability admin status back to its former value (NO + DRNO) .
		a. Login to new primary SDS GUI as admin user
		b. Select [Main Menu: Administration → General Options]
		c. Set *durableAdminState* to 3 (NO + DRNO)
		d. Click the 'OK' button
		2. Now new DR SDS servers are part of provisioning database durability.

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, please execute Step 8 on new-Primary SDS (old-DR SDS) and step 2 on new-DR SDS (old-Primary SDS) of this procedure.

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

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. Navigate to GUI screen [**Main Menu: Status & Manage → KPIs**] and select 'DP' tab. 2. Verify that 'Total Queries/Sec' KPI is now showing '0' for this DP server.
4 ▪	Replace the defective DP server	1. Power down the defective DP server 2. Label all connected cables. 3. Disconnect all necessary cables so the defective DP server can be physically removed from the enclosure for replacement. 4. Follow reference [10], BL460cc Hardware Upgrade, to remove and replace the DP blade. 5. Wire in the new DP blade server according to the cables you labeled and removed from the old blade.
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 37 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 B**
8 ▪	Restart the application on the new DP server	Execute procedure 10, steps 85 trough 89 (Restarting the application on the new DP server) as described in reference [1]
9 ▪	Verify status and traffic.	1. Using VIP address, login to SOAM GUI site where DP is located. 2. Navigate to GUI screen [**Main Menu: Status & Manage → KPIs**] and select 'DP' tab. 3. Verify that 'Total Queries/Sec' KPI is now showing a non-zero value for this DP server.

2.2.3 Post Condition

- DP server is processing traffic

2.3   Replacement of a SOAM Server

2.3.1   Pre Condition

- SOAM serevr 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

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 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 ☐	Remediate hardware and Recover DSR services	Execute Recovery Scenario 2, of reference [4], DSR Disaster Recovery Guide, to remediate hardware and restore DSR blade services.
5 ☐	Install SDS application on he 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 48, 51 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 27 through 31 (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

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. Follow reference [5] for the physical installation of the new Query server and reconnect all network cables you labeled and removed from the old server. 5. Power up the new Query server
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 2, steps 25 through 50 (Applying TKLCConfigData.sh file on the new Query server) as described in reference [1].
6 ☐	Add the new Query server back to SDS server group	1. Navigate to GUI screen [**Main Menu: Configuration → Server Groups**] 2. Select SDS server group of Query server 3. Click the "Edit" button. 4. Under "SG Inclusion", check the box for the Query server 5. Click the "OK" button.
7 ☐	Restart the application on the new Query server	1. Navigate to GUI screen [**Main Menu: Status & Manage → Server**] 2. Select the new Query server. 3. Click the "Restart" button. 4. In pop-up window, click the "OK" button to confirm

2.4.3   Post Condition

- Query server is back in service

2.5   Replacement of a SDS server

2.5.1   Pre Condition

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

2.5.2   Recovery Steps

1	Prepare for server replacement.	Identify the defective SDS server that needs replacement Defective SDS server hostname = _____
2	Make the defective SDS 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 server to 'Standby' 5. Click OK button
3	Remove SDS 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 server 5. Click the "OK" button.
4	Power down and replace SDS Server	1. Power down the defective SDS server. 2. Label all cables connected to the defective SDS server. 3. Physically remove the defective SDS server from the frame 4. Follow reference [5] for the physical installation of the new SDS server and reconnect all network cables you labeled and removed from the old server. 5. Power up the new SDS server
5	Install the SDS application on new SDS server	Execute Procedure 1 (Installing the SDS Application) from reference [1].
6	Prepare SDS server	Execute procedure 2, steps 25 through 50 (Applying TKLCConfigData.sh file on the new SDS server) from reference [1].
7	Add the new SDS server back to the server group	6. Navigate to GUI screen [**Main Menu: Configuration → Server Groups**] 7. Select SDS's server group. 8. Click the "Edit" button. 9. Under "SG Inclusion", check the new SDS server 10. Click the "OK" button.
8	Restart the application on new SDS server	. Navigate to GUI screen [**Main Menu: Status & Manage → Server**] 2. Select the new SDS server. 3. Click the "Restart" button. 4. In pop-up window, click the "OK" button to confirm

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)	5. Execute steps as described in **Appendix C**

2.5.3   Post Condition

- SDS server is back in service

2.6   Replacement of Primary SDS server pair

2.6.1   Pre Condition

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

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

2.6.2   Recovery Steps

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.
2 ☐	Power down and remove all defective Primary SDS servers. Replace them with new SDS servers.	2. Power down all defective SDS servers. 3. Label all cables connected to defective SDS servers. 4. Physically remove defective SDS servers from the frame. 5. Follow reference [5] for the physical installation of new SDS servers. 6. Wire in the new SDS servers according to the cables you labeled and removed from the old servers.
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. Copy the uncompressed backup archive files identified in step 1 to `/var/TKLC/db/filemgmt` area on newly installed Primary SDS-A server.
		3. Execute this command to stop running applications. Leave database running.
		`prod.stop`
		4. Restore the configuration DB by executing this command
		`idb.restore -n -t /var/TKLC/db/filemgmt -v <full path to configuration archive file name>`
		5. Restore the provisioning DB by executing this command:
		`idb.restore -n -t /var/TKLC/db/filemgmt -v <full path to provisioning archive file name>`
		6. SDS database is now restored. Start application by executing
		`prod.start`

6 ☐	Prepare the new Primary SDS-A server	Execute procedure 2, steps 25 through 50 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 25 through 50 on the new Primary SDS-B server (Applying TKLCConfigData.sh file) from reference [1].
9 ☐	Install the SDS application on the new Primary SDS Query server	Execute Procedure 1 on the new Primary SDS Query server (Installing the SDS Application) from reference [1].
10 ☐	Prepare the new Primary SDS Query server	Execute procedure 2, steps 25 through 50 on the new Primary SDS Query server (Applying TKLCConfigData.sh file) from reference [1].
11 ☐	Restart the application on all new Primary SDS 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 avove for Primary SDS-B server, and Primary SDS Query server
12 ☐	Install Netbackup Client Software on Primary SDS-A and Primary SDS-B servers (optional)	Execute steps as described in Appendix C
13 ☐	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

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.	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. Click "Inhibit Replication" button for each defective SOAM servers identified in the above step 1
3 ☐	Remediate hardware and Recover DSR services	If DSR recovery has not already been performed, execute Recovery Scenario 2, of reference [4], DSR Disaster Recovery Guide**.**
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 ☐	Prepare the new SOAM-A server	Execute Procedure 8, steps 45 through 48, 51 through 74 (Applying TKLCConfigData.sh file on SOAM server) from reference [1]
6 ☐	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].
7 ☐	Prepare the new SOAM-B server	Execute Procedure 8, steps 45 through 48, 51 through 74 (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. Click "Allow Replication" button for each newly replaced SOAM-A and SOAM-B servers 6. 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 27 through 31 (Restarting application on SOAM server) from reference [1].
10 ☐	Restart the application on the new SOAM-B server	Execute procedure 9, steps 27 through 31 (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.

2.7.3   Post Condition

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

2.8   Replacement of DR SDS 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 servers
- New DR SDS servers for replacement are available
- Access to Primary SDS GUI is functional

2.8.2   Recovery Steps

1 ☐	Prepare for server replacement.	Identify the DR SDS 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 servers. Replace them with new servers.	1. Power down all defective DR SDS servers. 2. Label all cables connected to defective DR SDS servers. 3. Physically remove defective DR SDS servers from the frame. 4. Follow reference [5] for the physical installation of new SDS servers. 5. Wire in the new DR SDS servers according to the cables you labeled and removed from the old servers.
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 2, steps 25 through 50 on the new DR SDS-A server (Applying TKLCConfigData.sh file) 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 2, steps 25 through 50 on the new DR SDS-B server (Applying TKLCConfigData.sh file) 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 2, steps 25 through 50 on the new Query server (Applying TKLCConfigData.sh file) from reference [1].
9 ☐	Restart the application on all new DR SDS 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 DR SDS-A server 4. Click the "Restart" button 5. In pop-up window, click the "OK" button to confirm Repeat all avove for DR SDS-B server, and DR SDS Query server

10 ☐	Install Netbackup Client Software on DR SDS-A, and DR SDS-B servers (optional)	Execute steps as described in Appendix C
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**] 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 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 servers and a Query Server is available
- DR SDS servers are available
- Access to DR SDS GUI is functional

2.9.2   Recovery Steps

1 ☐	Determine SDS site and status of provisioning	If the destroyed SDS frame was the Primary SDS frame, then execute procedure from **Section 2.1** 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 servers in new DR SDS frame	Install new DR SDS servers into new DR SDS frame by following instructions in reference [5].
4 ☐	Install switches in new DR SDS frame	Install new switches into new DR SDS frame by following instructions in reference [5]
5 ☐	Connect DR SDS servers	Wire in the new DR SDS servers by following instructions in reference [8].
6 ☐	Recover DR SDS 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

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

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. DISABLE HYPERTHREADING

This section is to be run only once on each DP; the configuration stays across future upgrades. If hyperthreading was disabled during installation, it is not be required to be executed again. Disable hyperthreading applies only to DP servers.

Appendix B: Disable Hyperthreading

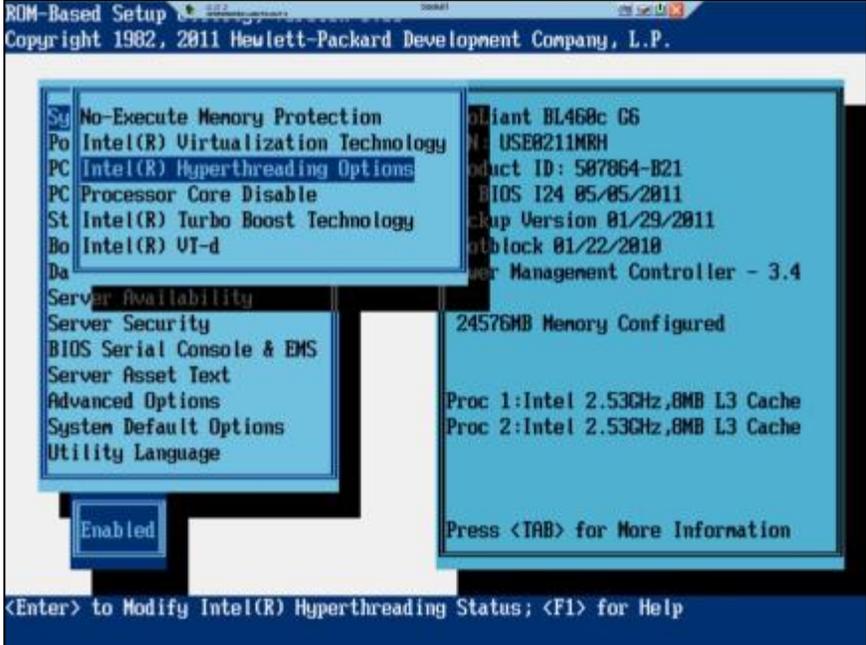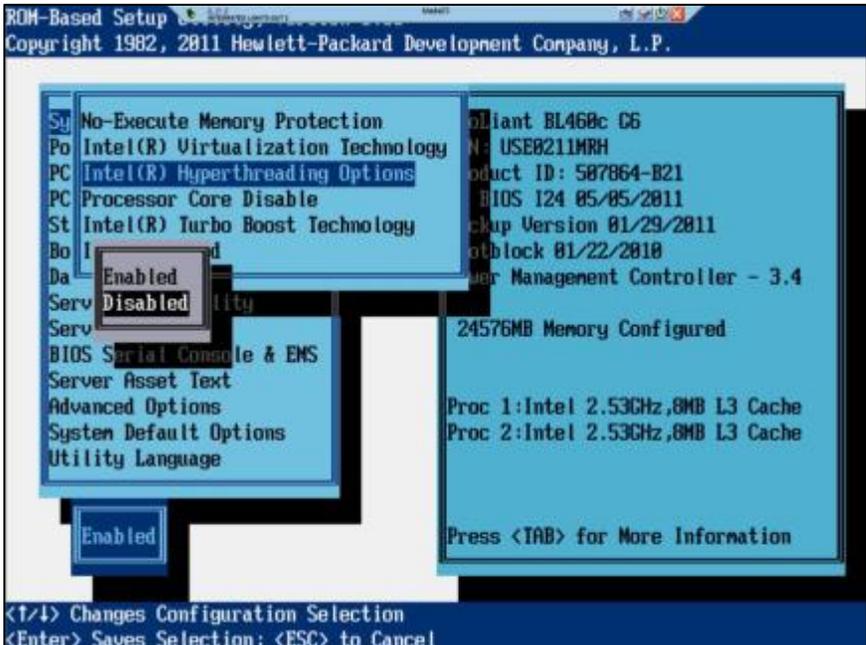| Step	Procedure	Result
1. ☐	**DP Server XMI IP (SSH):** Log into the server as the **admusr**	`login: admusr` `Password: <admusr_password>`
2. ☐	**DP Server XMI IP (SSH):** Switch to the **root** user	`# sudo -s`

3. ☐	**DP Server XMI IP (SSH):**
	
	Check the number of expected CPUs.
		`# syscheckAdm system cpu --get --var='EXPECTED_CPUS'`
		`39`
		
		NOTE: If the number is greater than 20, then this procedure has not been run before.

	📝	**NOTE: If the number of CPUs is reported as 20, this procedure has already been run for this DP. You may return to the calling section.**
4. ☐	**DP Server XMI IP (SSH):** Set the number of expected CPUs to the number of physical CPUs (20 for BL360 hardware).	`# syscheckAdm system cpu --set --var='EXPECTED_CPUS' --val='20'`
5. ☐	**DP Server XMI IP (SSH):** Verify the set number of expected CPUs.	`# syscheckAdm system cpu --get --var='EXPECTED_CPUS'` `20`

6. ☐	**DP Server XMI IP (SSH):**
	
	Restart sycheck service.
		`# stop syscheck`
		`syscheck stop/waiting`
		
		`# start syscheck`
		`syscheck start/running, process 48790`

7. ☐	**DP Server XMI IP (SSH):**
	
	Verify the number of CPUs recorded at OS installation.
		`# cat /usr/TKLC/awpcommon/prod/bin/NumOriginalCpus`
		
		`40`
		
		NOTE: If a "No such file or directory" response is received, then skip to **Step 10** of this procedure.

Appendix B: Disable Hyperthreading

Step	Procedure	Result
8. ☐	**DP Server XMI IP (SSH):** Modify the number of CPUs recorded at OS installation to **"20"**.	`# echo 20 > /usr/TKLC/awpcommon/prod/bin/NumOriginalCpus`

9. ☐	**DP Server XMI IP (SSH):**
	
	Verify the number of CPUs has been updated to **"20"**.
		`# cat /usr/TKLC/awpcommon/prod/bin/NumOriginalCpus`
		
		`20`

10. ☐	**DP Server XMI IP (SSH):** Reboot the DP server	`# init 6`
11. ☐	Access the Server BIOS	Reboot the server. This can be achieved by pressing and holding the power button until the server turns off, then after approximately 5-10 seconds press the power button to enable power. As soon as you see **F9=Setup** in the lower left corner of the screen, press **[F9]** to access the BIOS setup screen. You may be required to press [F9] 2-3 times. The F9=Setup will change to F9 Pressed once it is accepted. See example below. **Expected Result:** • ROM-Based Setup Utility is accessed and the ROM-Based Setup Utility menu will be displayed.
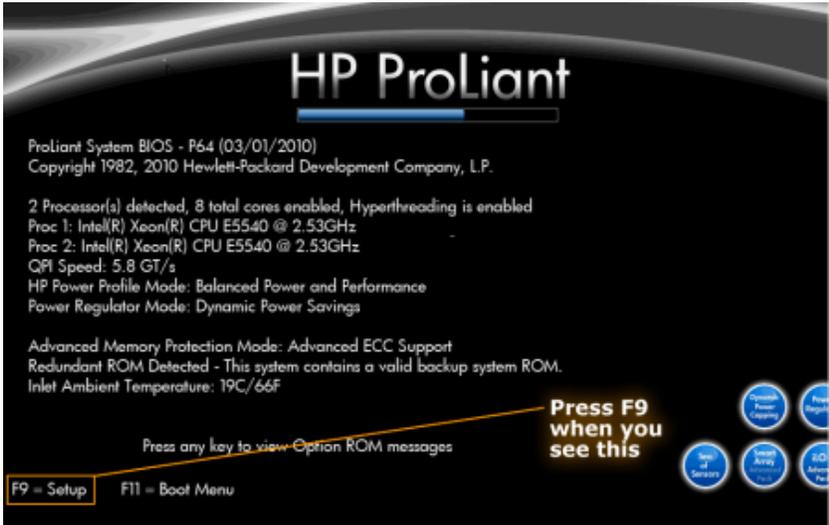
Appendix B: Disable Hyperthreading

Step	Procedure	Result
12. ☐	Select System Options	Scroll to **System Options** and press **[ENTER]**
13. ☐	Select Processor Options	Select **Processor Options** option and press **[ENTER]**
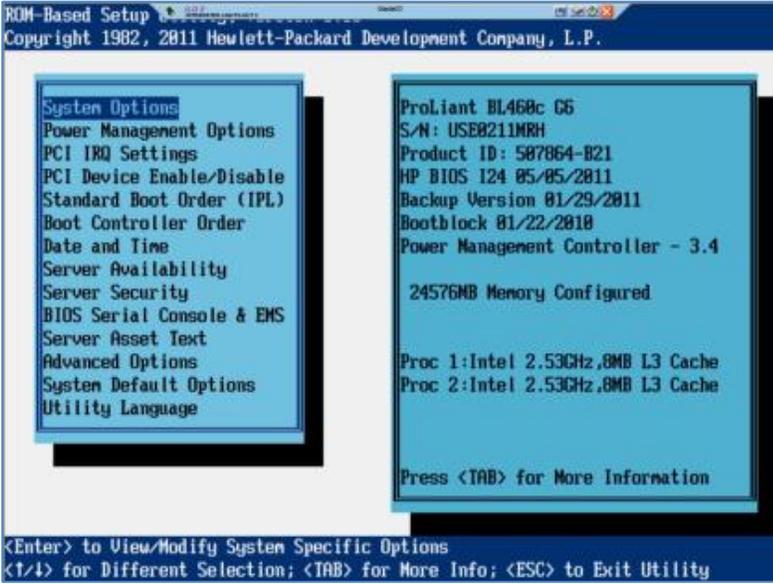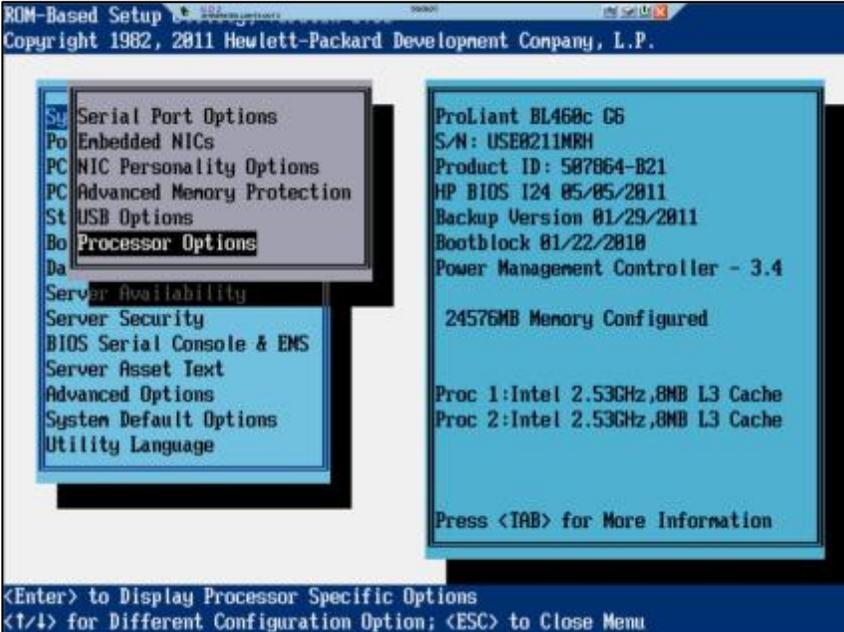
Appendix B: Disable Hyperthreading

Step	Procedure	Result
14. ☐	Select Hyperthreading Options	Select **Intel® Hyperthreading Options** option and press **[ENTER].**
15. ☐	Set hyperthreading to **Disabled**.	Select **Disabled** option and press [ENTER]**.**

Appendix B: Disable Hyperthreading

Step	Procedure	Result
16. ☐	Save the configuration and exit	Press [F10] key to save the configuration and exit. The server will reboot ROM-Based Setup Utility, Version 3.00 Copyright 1982, 2010 Hewlett-Packard Development Company, L.P. System Options Power Management Options PCI IRQ Settings PCI Dev... Standar... <F10> to Confirm Exit Utility Boot Co... Date and Time Server Availability Server Security BIOS Serial Console & EMS Current Boot Controller PCI Embedded HP Smart Array P410i Controller Utility Language HP ProLiant DL360 G6 S/N: USE013N1C7 Product ID: 484184-B21 HP BIOS P64 03/01/2010 Backup Version 03/01/2010 Bootblock 06/20/2009 Power Management Controller - 2.9 24576MB Memory Configured Press <TAB> for More Information **Expected Result:** • Settings are saved and server reboots.
	THIS PROCEDURE HAS BEEN COMPLETED	

Appendix C. INSTALL NETBACKUP CLIENT

Appendix C: Disable Hyperthreading

Step	Procedure	Result

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: Neetbackup client software must be installed on each SDS 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	