Oracle® Communications Subscriber Data Management

Installing SPR 9.0 on DL380

Release 9.0

E63816-01

November 2012

ORACLE®

Oracle Communications Subscriber Data Management, Installing SPR 9.0 on DL380, Release 9.0

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

My Oracle Support (MOS) (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.
Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.
See more information on MOS in the Appendix section.

Table of Contents

List of Figures

List of Tables

1.0 PURPOSE AND SCOPE

The purpose of this document is to document the installation of SDM 9.0.0 software on theTPD 5.2.1 Linux environment, on DL380 G8 hardware.

This document is intended for Oracle field personnel who need to install SDM software on DL380 hardware running TPD.This document may be used in discussions with the customer to determine if this product satisfies their expectations. The reader is assumed to be familiar with TPD and DL380 servers, and this document focuses on the specifics of the installation unique to an SDM/SPR installation in a TPD environment.

1.1 ACRONYMS

Acronym	Description
ILO	Integrated Lights Out manager
SDM	Subscriber Data Management
TPD	Oracle Platform Distribution
SDM1	SDM C-CLASS Servers located on site 1
SDM2	SDM C-CLASS Servers located on site 2
OA	HP Onboard Administrator
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform

Table 1: Acronyms

1.2 REFERENCES

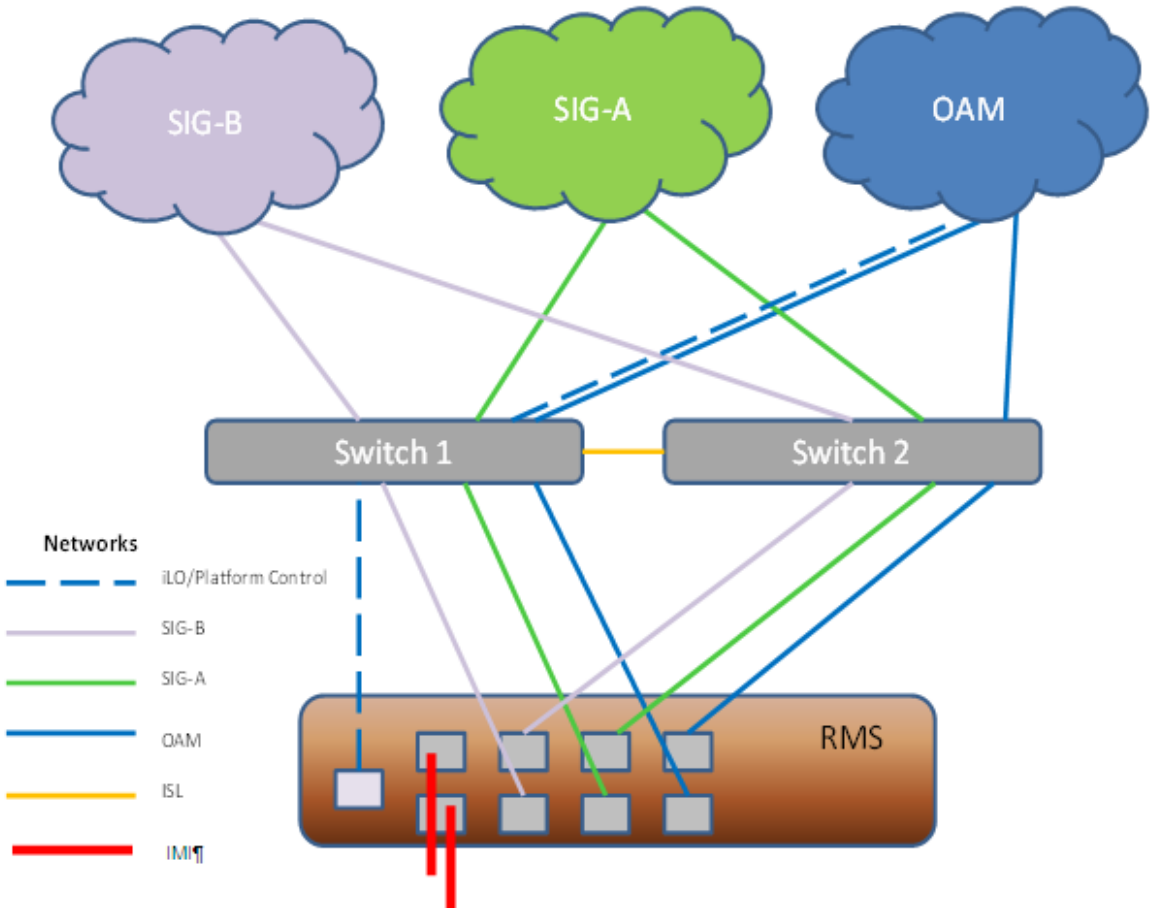
Ref ID	Part Number	Title	Version
[TK1]	909-1620-001	Platform 4.x HP G8 Configuration Procedure Reference	Rev F 2012
[TK2]	910-6611-001	“HP Solutions Firmware Upgrade Pack, Upgrade Procedures 2.3”, Section 4.8	
[TK3]	910-6611-001	HP Solutions Firmware Upgrade Pack 2.2.3, Release Notes”	
[TK4]	PD001866	Formal Peer Review Process	Rev 16.0
[TK5]	TR006928	SDM Advanced Routing for Virtual IP addresses (VIPs)	
[TK6]	TR007093	SDM NetBackup configuration	

Table 2: References

1.3 HIGH LEVEL FUNCTIONAL DESCRIPTION

In a typical small installation of SDM software, two DL380 servers are installed with TPD Linux followed by SDM SPR software.

Figure 1: SPR on DL380 Connectivity figure



1.4 INSTALLATION RESTRICTIONS

The TPD software version combination for which this installation procedure is applicable is the following:

- TPD 5.0.1-73.3.0 x64 + SDM 9.0.0

1.5 INSTALLATION PREREQUISITES

In order to complete this installation, you should have the following:

- The DL380 servers used have two on-board Ethernet ports and the minimum number of ports required for a 2-server TPD/SDM installation is five Ethernet ports.
- A valid recent **TPD 5.0.1-73.3.0 x64** release of TPD 64-bit must be on. This must be available either in CD/DVD format or on a Windows PC that has network access to the ILO network ports of the DL380 servers.
- The TPD ISO file available on a Windows PC, connecting to the ILO in HTTP with Internet Explorer from the PC will allow using the Virtual Media feature to make the file appear as a CD mounted in the CD/DVD drive.
- A valid recent 9.0.0 release of SPR software must be on hand. This should be a n iso image format with a filename 872-2409-101-9.0.0_5.0.0-SDM-x86_64.iso
- The script named "`create_SDMdiskconfig.pl`" (included in SDM iso media)
- The HP Diameter license and SDM license codewords are needed
- The SDM SPR 9.0 Subscriber license file is needed
- **sdm-ssh.conf** file and **sdm-ssh-tool** script (included in SDM iso media)

1.5.1 Networks List in DL380 rack mount server

The table below shows a list of the networks used in the SDM configuration on DL380 servers (SDM Server A and Server B):

Network Name	Identifier	Default VLAN ID	Subnet Size, Mask	Routable	Usage
Management	PlatMgt[1]	-	/26	Yes	Management and ILO
OAM/Geo	XMI	-	/27	Yes	External management access and Geo redundancy replication
Internal Messaging	IMI	-	/16	No	Internal Communication Network - Requires 2 static IPs (fixed to 169.254.0.0/16)
Signaling – A	XSI-1	-	/28	Yes	First External Signaling Network
Signaling – B	XSI-2	-	/28	Yes	Second External Signaling Network

Table 3*:* Network List in DL380 server

Note: *In this procedure vlans are not used.*

If using vlans:

vlans must be added from the platcfg menu in the interface configuration.
The vlan ids must be populated in the sdm-vlans.conf file

- The two DL380 servers should have their ILO Ethernet ports plugged in, configured, and accessible over the MGMT_NET network, with their IP addresses known (ILO_IP_ADDR_1, ILO_IP_ADDR_2)

- The network configuration needed for the OAM connection to the customer network XMI should be known.

1.5.2 XMI configuration

○ XMI Subnet number:	XMI_Subnet
○ XMI Subnet mask:	XMI_MASK
○ XMI Default gateway:	XMI_GATEWAY
○ XMI Planned IP addresses of SDM servers: (must be local to XMI)	XMI_SDM_IP
○ Planned host name of SDM servers:	XMI_SDM_Hostname
○ At least one planned VIP for SDM: (must be local to XMI, could be an OA&M VIP for example)	XMI_SDM_VIP
○ Two planned VIP for Geo redundancy proposes : ○ Geo_SDM1_VIP ○ Geo_SDM2_VIP	

Table 4: XMI Configuration

[1] Note that choosing the minimum required subnet size might minimize the option of co-mingling with other applications in the same frame.

1.5.3 Traffic or XSI-1 configuration

- The network configuration needed for the traffic connection to the customer network XSI-1 :

○ XSI-1 Subnet number:	XSI-1_Subnet
○ XSI -1Subnet mask:	XSI-1_MASK
○ XSI-1 Default gateway:	XSI-1_GATEWAY
○ XSI-1 Planned IP addresses of SDM servers:	XSI-1_SDM_IP

Table 5: XSI-1 configuration

1.5.4 Traffic or XSI-2 configuration

Eventually the network configuration needed for the second traffic connection to the customer network XSI-2 should be known:

○ XSI-2 Subnet number:	XSI-2_Subnet
○ XSI -2 Subnet mask:	XSI-2_MASK
○ XSI-2 Default gateway:	XSI-2_GATEWAY
○ XSI-2 IP addresses of SDM servers:	XSI-2_SDM_IP

Table 6: XSI-2 configuration

1.5.5 NTP

At least one time synchronization NTP server IP address which is accessible through the XMI network should be known: NTP_IP

1.5.6 Adding Private Network

The TPD/SDM servers need to communicate together on an IP subnet that is private (169.254.0.0/16). Such a small subnet that does not conflict with the customer network must have been selected:

Description	**IP**
IMI Subnet number	169.254.0.0
IMI Subnet mask	255.255.0.0
IMI IP Address for SDM Server 1	169.254.1.1
IMI IP Address for SDM Server 2	169.254.1.2

Table 7: IMI configuration

1.5.7 Adding Additional Parameters

SDM software requires additional networking parameters for its operation. All these parameters must be specified in file **/etc/sysconfig/blue** on each SDM/TPD server:

Description	**Information**
SDM site Name	SDM_CUSTOMER_SITE_NAME
SDM SRP communication Domain	SDM_CUSTOMER_SRP_DOMAIN
For each SDM/TDP server, a slot ID	SDM_UNIQUE_SLOT_ID

Description	Information
(a unique integer in the range 1-16)	

1.6 AUTHENTICATION

1. The usernames and passwords that can login to the ILO in full privilege mode should be known. On a DL380 server coming straight from the factory, the initial ILO username/password is of the server is written on a little pull-out tab located left of the left-most hard-drive bay of the unit.
2. The default password of the “root” account of the Oracle TPD installation must be known to the installer.
3. The default password of the “admin” account of the Oracle SDM installation must be known to the installer.

The DL380 servers will be called SDM Server A and Server B where Server A designate the Active system controller and Server B the standby System controller. Furthermore, as Geo redundancy is used SDM1 and SDM2 will be used for SDM Server A and Server B located on site 1 and SDM Server A and Server B located on site 2.

1.7 BASIC INSTALLATION OF TPD

This installation should be repeated for C-CLASS on all blades on both sites (SDM1 and SDM2) planned to be part of the SDM/TPD configuration.

1.8 VERIFY ILO SETTINGS ON SDM SERVER A AND SERVER B

- Connect to the DL380 ILO using HTTP from a Windows PC running Internet Explorer that has the TPD ISO available, and use the Virtual Media option of the ILO to make the TPD ISO file from the Windows PC available as a boot image to the DL380 (as if it was in the CD-ROM drive).

1.9 DL380 CONFIGURATION WITH ADDITIONAL DRIVES

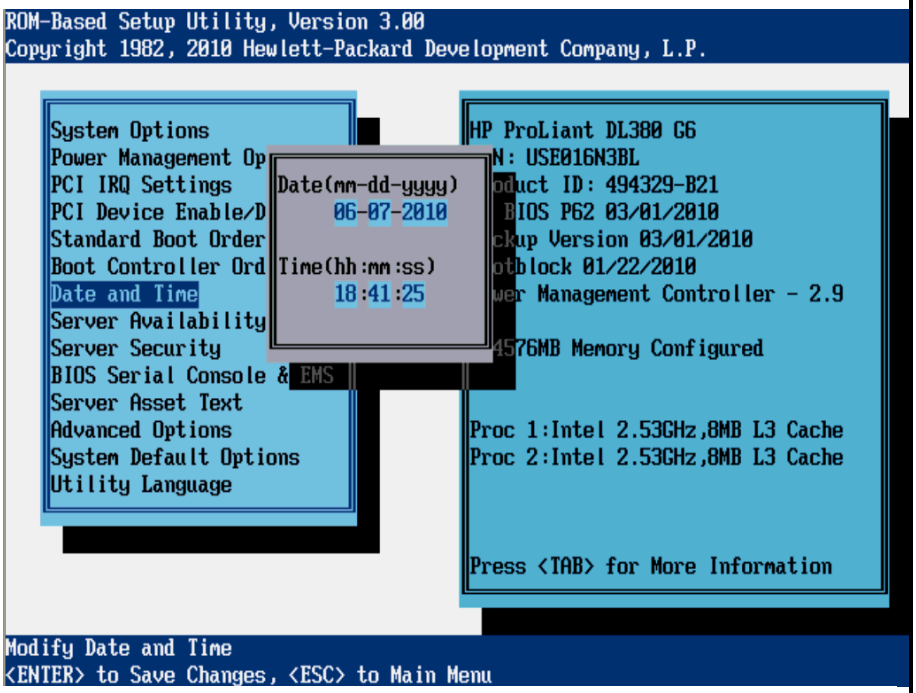
Hardware Configuration		Servers/site	RAM /server	HD /server (BE)
2302	2x DL380-64GB RAM 2x600GB HDD	2	48GB	2x 600GB in RAID1
2352	2xDL380-64GB RAM 2x600GB HDD 6 additional 600GB HDD	2	64GB	4x (2x 600GB in RAID1)
2552	2xDL380-128GB RAM 2x600GB HDD 6 additional 600GB HDD	2	128GB	4x (2x 600GB in RAID1)

Table 8: DL380 HW configuration types

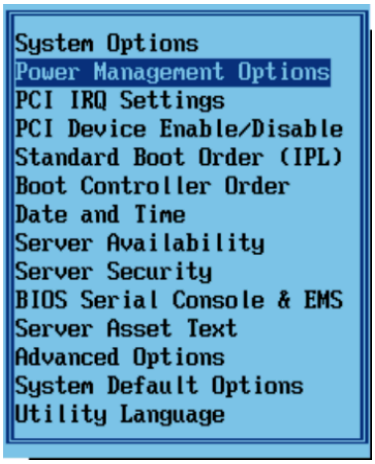
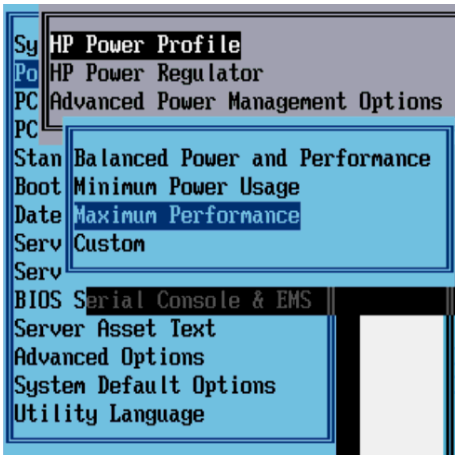
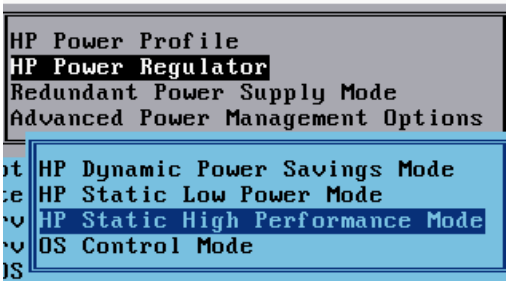
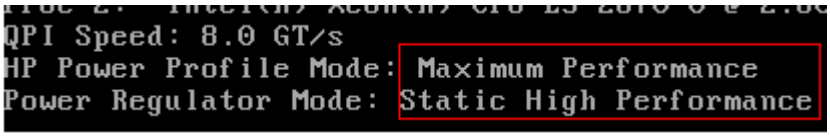
If the SPR configuration to be used is 2352 or 2552 (8 hard drives in 4 x (2HDD in RAID1)) 6 extra HD of 600GB are needed.

2.0 ADJUST POWER MANAGEMENT AND INSTALL TPD

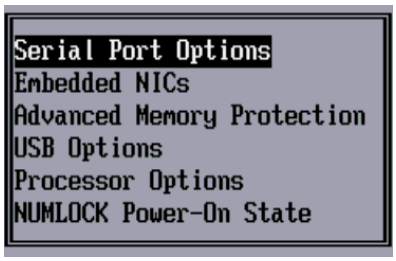
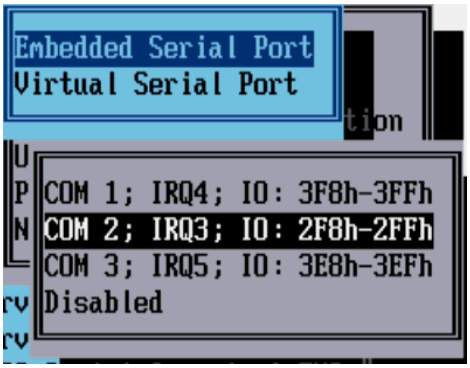
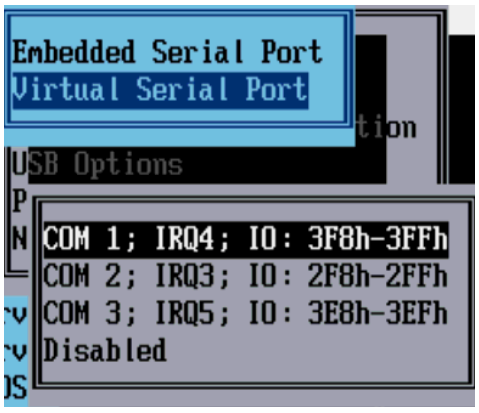
Procedure 1. This procedure install TPD on DL380

S T E P #	This procedure will install TPD on DL380 server **Needed material:** - TPD iso Media Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	Connect to the Server	Connect to the Server using a VGA Display and USB Keyboard, or via the iLO interface using IE.
2 ☐	Insert TPD Media into Server	Insert TPD media in the optical drive. (You can also attach the TPD ISO to the iLO) .
3 ☐	Access the Server BIOS	Reboot the server and after the server is powered on, as soon as you see **<F9=Setup>** in the lower left corner of the screen, press **F9** to access the BIOS setup screen.
4 ☐	Set CMOS Clock	Scroll to *Date and Time* and press **Enter** Set the date and time and press **Enter**, the time zone to be used is UTC. 

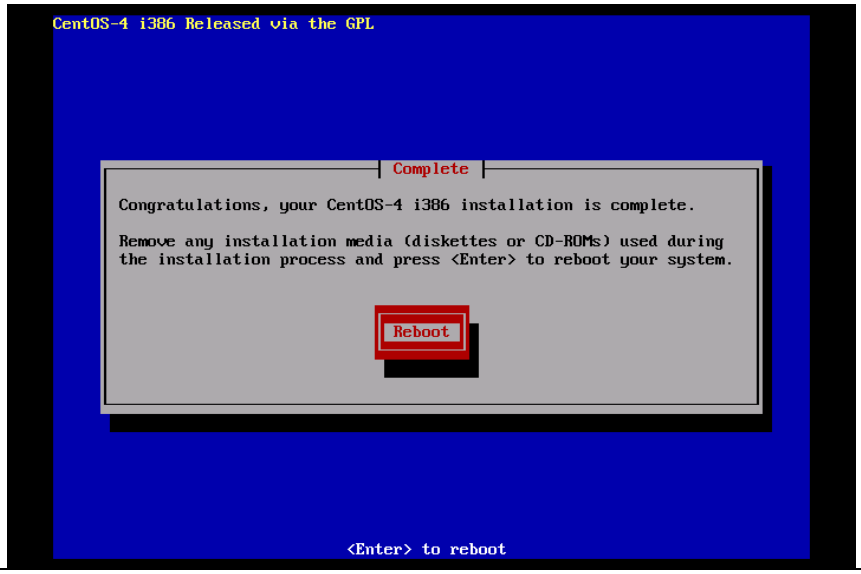
Procedure 1. This procedure install TPD on DL380

5 ☐	Adjust Power Management Options	Go back to the main menu by pressing **<Esc>** and scroll down to *Power Management Options* and press **Enter** Select *HP Power Profile* and press **Enter** Scroll down to *Maximum Performance* and press **Enter**   Press **<Esc>** to return to the main menu *Under Management Options* press **Enter** Select *HP Power Regulator* and press **Enter** Scroll down to *HP Static High Performance Mode* and press **Enter**  theses parameters can be checked At server boot : 

Procedure 1. This procedure install TPD on DL380

5 ☐	Configure iLO Serial Port	Scroll to *System Options* and press **Enter** **Change power profile (same as blades)** Select *Serial Port Options* and press **Enter**  Press **Enter** to select *Embedded Serial Port* and change it to *COM2* and press **Enter**  Press **Enter** to select *Virtual Serial Port* and change it to *COM1* and press **Enter**  Press **<ESC>** 2 times to return to the main menu

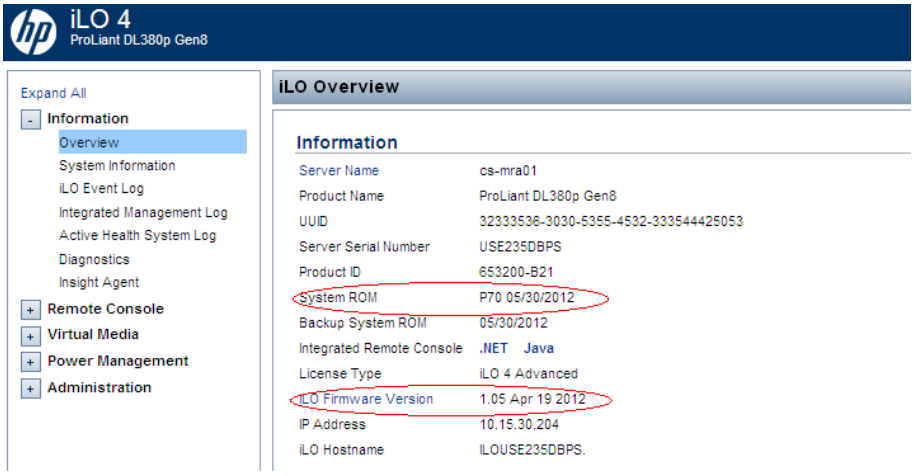
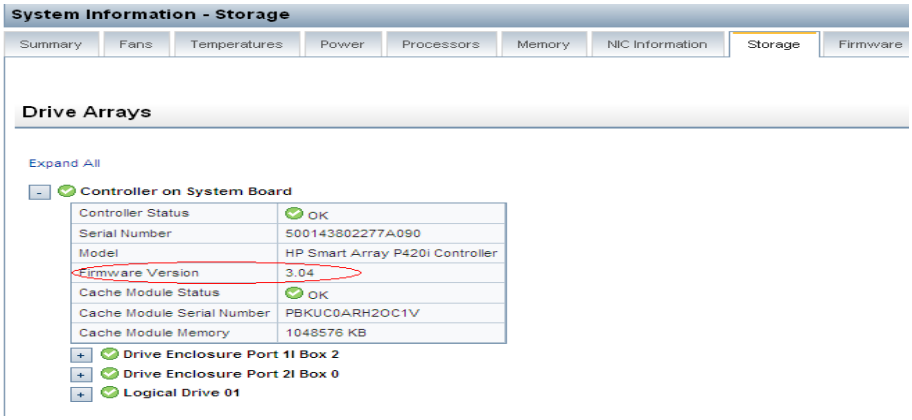
Procedure 1. This procedure install TPD on DL380

6 ☐	Double Check boot Order.	Scroll to *Standard Boot Order* and press **Enter** Verify that the first boot device is set to *CD-ROM*, if not, set CD-ROM to be the first boot device and press **Enter** Press **<ESC>** to return to the main menu.
7 ☐	Save Configuration and Exit	Press **<ESC>** then press **F10** to save the configuration and exit. The server will reboot
8 ☐	Begin IPM Process	Once the Server reboots, it will reboot from the TPD media and a boot prompt shall be displayed. IPM the server using the following command: For DL380 Gen8 **`TPDnoraid diskconfig=HPHW,force console=tty0 PrimaryConsole=tty0`**
9 ☐	IPM Complete	The IPM process takes about 30 minutes, you will see several messages and screens in the process. Once the IPM is complete, you will be prompted to press Enter as shown below. Remove the disk from the drive or unmount the TPD image from the iLO and press **Enter** to reboot the server. Note that the CD may eject automatically. 
10 ☐	Server Reboot	Once the Server Reboots, you should see a login prompt. Note that during the first system boot, swap files may be initialized and activated. Each swap file will take about 2 minutes. If no login prompt is displayed after waiting 15 minutes, contact Oracle Customer Support for Assistance.

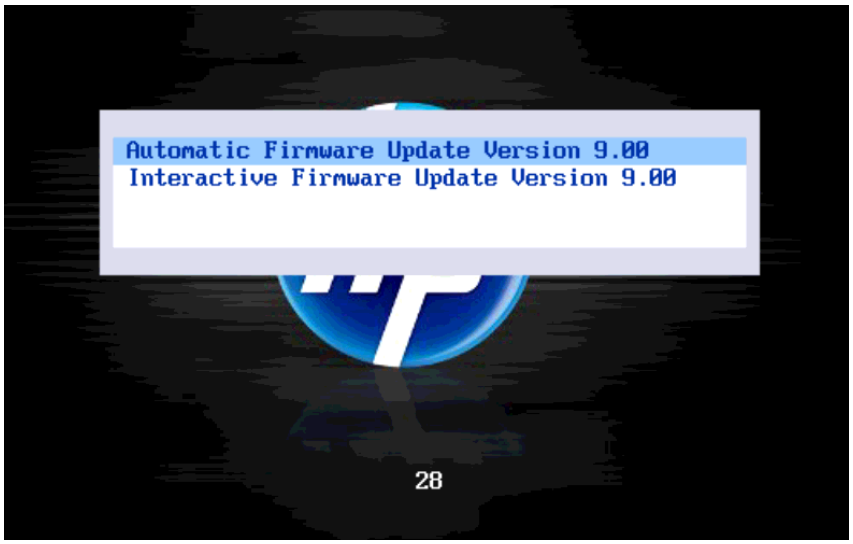
3.0 UPGRADE DL380 SERVER FIRMWARE

Procedure 2. Upgrade DL380 Server Firmware

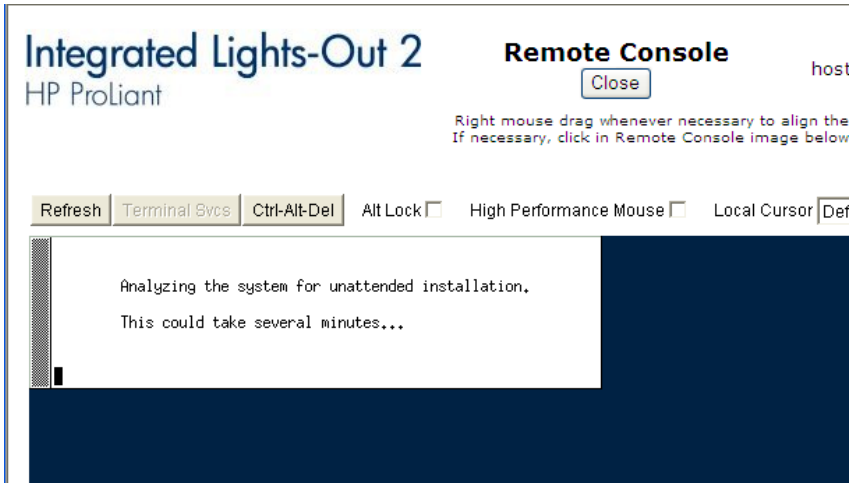
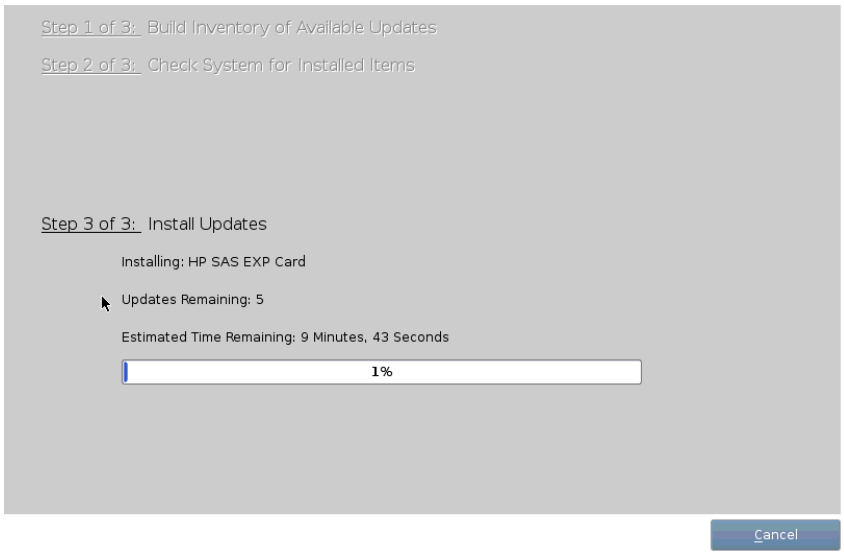
S T E P #	This procedure will upgrade the DL380 server firmware **Needed material:** - HP Firmware Maintenance CD/DVD - HP Solutions Firmware Upgrade Pack Release Notes [1] Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	Connect to the Server Console	Connect to the Server Console: - using a VGA Display and USB Keyboard, or - using the Server iLO port and iLo Web Interface (to access Remote Console) (Note: default IP address on the iLo port is _192.168.100.5_) Appendix B explains how to access the server iLO and set iLo IP address if necessary.

2. ☐	Optional: Determine current Firmware Revs	From the iLo, determine the current Firmware rev of the Server ROM and iLo. (Optional – since the Smart Update can be applied even if the firmware is already up-to-date.) Compare to latest Firmware Release notes. If firmware is up-to-date, the remainder of this procedure can be skipped. [Note: you still need to determine if any Errata (Firmware Patches) need to be applied. See Firmware Release notes.  The server ROM can also be obtained using the following command : **[root@cs-SPR01 ~]# dmidecode | grep -A 5 "BIOS Information"** BIOS Information Vendor: HP **Version: P70** **Release Date: 05/30/2012** Address: 0xF0000 Runtime Size: 64 kB The server ROM can also be obtained using the following command :  The RAID controller firmware version can also be obtained using the following command : **[root@cs-SPR01 ~]# hpacucli ctrl all show detail | grep Version** Firmware Version: 3.04

Procedure 2. Upgrade DL380 Server Firmware

3. ☐	server iLO: Prepare to upgrade DL380 server firmware	Insert HP Smart Update Firmware DVD into the removable media drive of the DL380 server. *Note: HP Smart Update Firmware may also be applied using a Virtual Mount on the iLo Web Interface.*
4. ☐	server iLO: Boot the server.	In the integrated remote console, log into the server as root if needed, and run: # **shutdown -r now**
5. ☐	Server Console:Perform firmware upgrade	The server will reboot into the *HP Smart Update Firmware* ISO and present the following boot prompt on the Console: Press **[Enter]** to select the **Automatic Firmware Update** procedure.  If no key is pressed in 30 seconds the system will automatically perform an Automatic Firmware Update.

Procedure 2. Upgrade DL380 Server Firmware

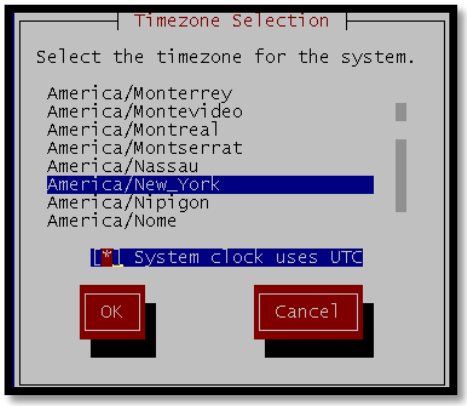
6. ☐	Server Console: System analysis	The firmware install will perform a system scan of the server in which it will identify all of the firmware components that are eligible for upgrade. This process may take up to 10 minutes and during that time the following screen is displayed on the console.  **Note**: No progress indication is displayed during the system scan and analysis stage. In about 10 minutes the installation will automatically proceed to the next step.
7. ☐	Console: Monitor installation	Once analysis is complete the installer will begin to upgrade the eligible firmware components. A progress indicator is display at this time as shown below.  **Note**: If the iLO4 firmware is to be upgraded it will be upgraded last. At this point the iLO4 session will be terminated and you will lose the remote console, virtual media and Web GUI connections to the server. This is expected and will not impact the firmware upgrade process.
8. ☐	Local Workstation:Clean up	Once the firmware updates have been completed the server will automatically be rebooted. At this time you may close the remote console and the iLO4 Web GUI browser session.

Procedure 2. Upgrade DL380 Server Firmware

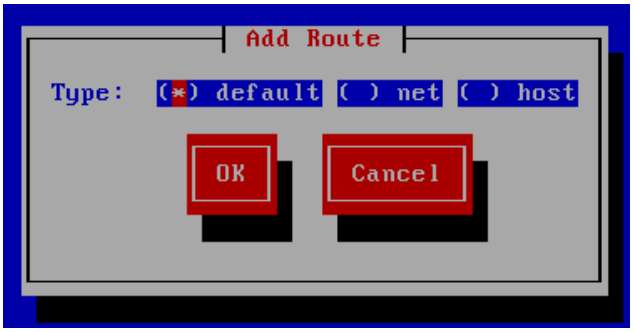
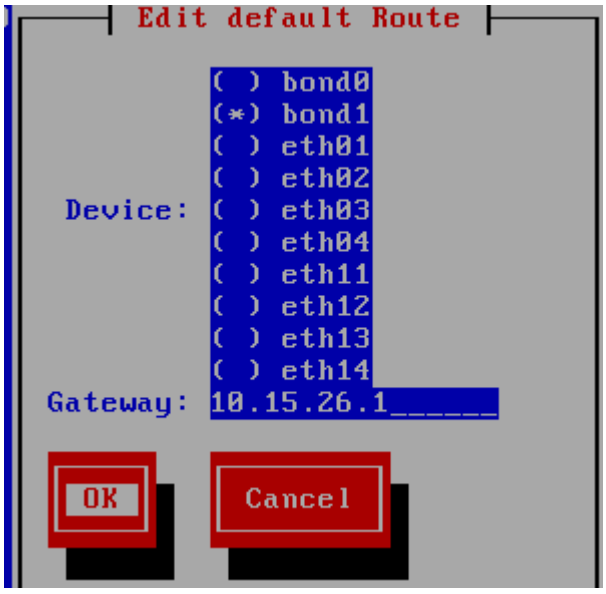
9. ☐	Local Workstation: Verify server availability	Wait 3 to 5 minutes and verify the server has rebooted and is available by gaining access to the login prompt.
10.	Local Workstation: Install firmware errata if any	IMPORTANT: It may also be necessary to "patch" the firmware, using a HP Provided "Firmware Errata". HP provides these patches for specific problems. See the HP Firmware Release notes for a list of available and required Errata, and the procedure to install these. The Errata are packaged as small executables that can be copied to the server, and executed. The errata are also easily installed remotely, if needed.
11. ☐	Management server iLO: Remove the firmware CD	Remove the HP Smart Update Firmware DVD from the removable media drive. Exit from the Integrated Remote Console.

4.0 BASIC POST INSTALL CONFIGURATION OF TPD ON EACH DL380 SERVER

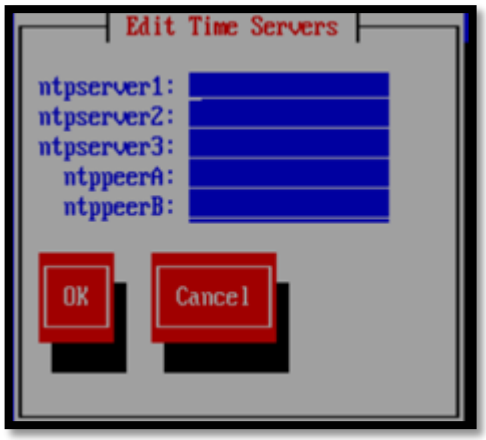
STEP #	Steps to be completed.	This installation must be repeated for each DL380 server planned to be part of the SDM/TPD configuration.It describes how to configure the network interfaces,NTP,RAID1 used by SDM SPR system. **Needed material:** - 6 Additional 600GB Physical Drives for DL380 configurations with 8 drives Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.
1 ☐	Edit network file on SDM Server A and Server B:	Using SSH or the Console of each DL380 server, login to the root account, and edit the file **/etc/sysconfig/network** to add the following line at then end of file: NOZEROCONF=yes The file content should look like: NETWORKING=yes NETWORKING_IPV6=yes HOSTNAME=hostnameNNNNN IPV6INIT=yes **NOZEROCONF=yes** Note: failing to do this step is going to trigger non immediate and difficult to identify problems that might prevent proper switchover, etc, because the blade won't be able to reach each other on the private network.
2 ☐	Change DL380 server hostname on SDM Server A and Server B	Use the TPD menu front-end to set the server's hostname to "XMI_SDM_Hostname": **# su - platcfg** navigate through Main Menu -> Server Configuration -> Hostname use the "Edit" button to change the Hostname from"hostnameNNNNNNNNNN" to "XMI_SDM_HOSTNAME" exit the menus, and verify that /etc/hosts is updated: **# grep 127 /etc/hosts** **127.0.0.1 localhost XMI_SDM_Hostname** **# su – platcfg** navigate through Main Menu -> Server Configuration -> Hostname

		use the "Edit" button to change the Hostname from"hostnameNNNNNNNNNN" to "XMI_SDM_HOSTNAME" Run the following command to reload the shell : **# exec bash** exit the menus, and verify that **/etc/hosts** file has been updated updated: **# grep 127 /etc/hosts** **127.0.0.1 localhost XMI_SDM_Hostname**
3 ☐	Change DL380 server Time Zone on SDM Server A and Server B	Use the TPD menu front-end to set the server's Time Zone: **# su - platcfg** navigate through Main Menu -> Server Configuration -> Time Zone use the "Edit" button to change the Time Zone navigate the menus back to the main menu and Exit  **The System Clock uses UTC, MUST BE SELECTED** • Verify the date : **# date**
4 ☐	Configure IMI interface (bonded) on SDM Server A and Server B	**Create virtual network interface bond0 (used for SDM inter-server communication on IMI) by combining eth01 and eth11**: **# netAdm add --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=30 --bootproto=none --primary=eth01** **# netAdm set --device=eth01 --bootproto=none--type=Ethernet --master=bond0 --slave=yes --onboot=yes** **# netAdm set --device=eth11 --bootproto=none --type=Ethernet --master=bond0 --slave=yes --onboot=yes** **# netAdm set --device=bond0 --address= IMI_SDM_TPD_IP_X --netmask= IMI_MASK --onboot=yes**

		• Verify the bond0 configuration: **# cat /proc/net/bonding/bond0** Ethernet Channel Bonding Driver: v3.4.0-1 (October 7, 2008) Bonding Mode: fault-tolerance (active-backup) Primary Slave: eth01 (primary_reselect always) Currently Active Slave: eth01 MII Status: up MII Polling Interval (ms): 30 Up Delay (ms): 0 Down Delay (ms): 0 Slave Interface: eth01 MII Status: up Speed: 1000 Mbps Duplex: full Link Failure Count: 0 Permanent HW addr: 2c:76:8a:52:eb:20 Slave Interface: eth11 MII Status: up Speed: 1000 Mbps Duplex: full Link Failure Count: 0 Permanent HW addr: ac:16:2d:80:2c:83  The IMI_SDM_IP adress must be 169.254.1.1 and 169.254.1.2 has to match exactly the SDM_UNIQUE_SLOT_ID value in /etc/sysconfig/blue file (in section 4.3 of the document)
5	Configure XMI interface on SDM Server A and Server B	• **Create virtual network interface bond1 (used for SDM connection to network XMI) by combining eth02 and eth12**: • Use netAdm command create bond1 **# netAdm add --device=bond1 --onboot=yes --type=Bonding --mode=active-backup --miimon=30 --bootproto=none --primary=eth02** • Use netAdm command top add eth01 and eth14 to bond1 **# netAdm set --device=eth02 --bootproto=none --type=Ethernet --master=bond1 --slave=yes --onboot=yes** **# netAdm set --device=eth12 --bootproto=none--type=Ethernet --master=bond1 --slave=yes --onboot=yes** **# netAdm set --device=bond1 --address= XMI_SDM_TPD_IP_X --netmask= XMI_MASK --onboot=yes** • Verify that bond1 interface is properly created : **# more /proc/net/bonding/bond1** *Bonding Mode: fault-tolerance (active-backup)* *Primary Slave: eth02 (primary_reselect always)* *Currently Active Slave: eth02*

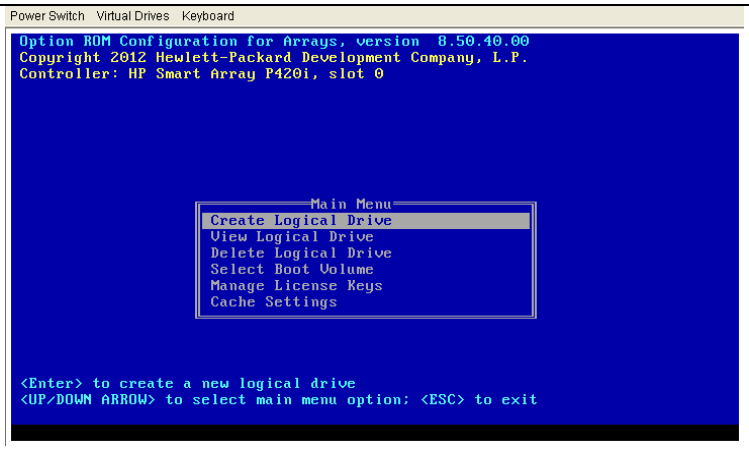
		MII Status: up ***MII Polling Interval (ms): 30*** *Up Delay (ms): 0* *Down Delay (ms): 0* ***Slave Interface: eth02*** *MII Status: up* *Speed: 1000 Mbps* *Duplex: full* *Link Failure Count: 0* *Permanent HW addr: 2c:76:8a:52:eb:21* ***Slave Interface: eth12*** *MII Status: up* *Speed: 1000 Mbps* *Duplex: full* *Link Failure Count: 0* *Permanent HW addr: ac:16:2d:80:2c:82*
6	Configure XMI gateway as the default route	• Use the TPD menu front-end to add a default route to gateway **XMI_GATEWAY**: **# su - platcfg** navigate through ***Main Menu -> Network Configuration -> Routing -> IPv4 -> Edit -> Add Route -> default***  

		• From this point, the TPD server should be reachable from the customer network XMI, so it is possible (if more convenient) to log out from the ILO virtual console and connect to the system with SSH to resume the installation. **# ping XMI_GATEWAY** *[root@CSLAB-SPR1-BLADE2 ~]# ping 10.15.26.1* *PING 10.15.26.1 (10.15.26.1) 56(84) bytes of data.* *64 bytes from 10.15.26.1: icmp_seq=1 ttl=255 time=0.733 ms* *--- 10.15.26.1 ping statistics ---* *1 packets transmitted, 1 received, 0% packet loss, time 0ms*
7 ☐	Configure XSI-1 interface on SDM Server A and Server B	Create virtual network interface bond2 (used for SDM connection to network XSI-1) by combining eth03 and eth13: Use netAdm command create bond1 **# netAdm add --device=bond2 --onboot=yes --type=Bonding --mode=active-backup --miimon=30 --bootproto=none --primary=eth03** Use netAdm command top add eth03 and eth13 to create bond2 **# netAdm set --device=eth03 --bootproto=none --type=Ethernet --master=bond2 --slave=yes --onboot=yes** **# netAdm set --device=eth13 --bootproto=none --type=Ethernet --master=bond2--slave=yes --onboot=yes** **# more /proc/net/bonding/bond2** *Bonding Mode: fault-tolerance (active-backup)* *Primary Slave: eth03 (primary_reselect always)* *Currently Active Slave: None* *MII Status: down* *MII Polling Interval (ms): 30* *Up Delay (ms): 0* *Down Delay (ms): 0* *Slave Interface: eth03* *MII Status: down* *Speed: 1000 Mbps* *Duplex: full* *Link Failure Count: 0* *Permanent HW addr: 2c:76:8a:52:eb:22* *Slave Interface: eth13* *MII Status: down* *Speed: 1000 Mbps* *Duplex: full* *Link Failure Count: 0* *Permanent HW addr: ac:16:2d:80:2c:81*
8 ☐	Configure XSI-2 interface (if needed) on SDM Server A and Server B	If a second traffic interface is to be used for the secondary Sh connection to the MPEs follow these steps :

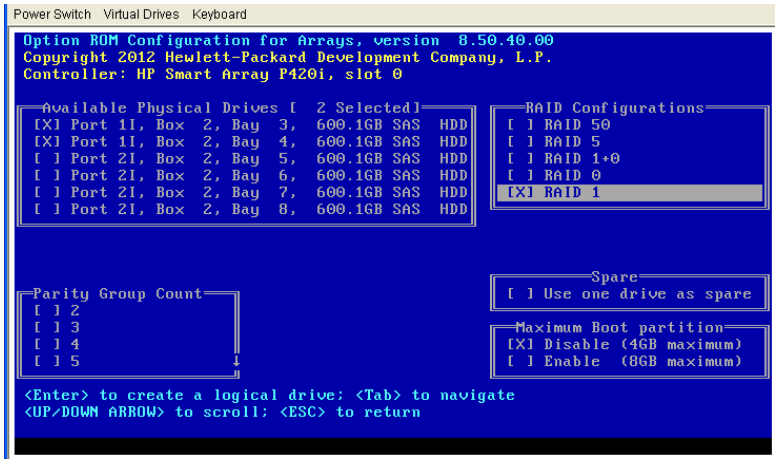
		Create virtual network interface bond3 (used for SDM connection to network XSI-1) by combining eth04 and eth14: Use netAdm command create bond1 **# netAdm add --device=bond3 --onboot=yes --type=Bonding --mode=active-backup --miimon=30 --bootproto=none --primary=eth04** Use netAdm command top add eth03 and eth13 to create bond2 **# netAdm set --device=eth04 --bootproto=none --type=Ethernet --master=bond3 --slave=yes --onboot=yes** **# netAdm set --device=eth14 --bootproto=none --type=Ethernet --master=bond3--slave=yes --onboot=yes** **# more /proc/net/bonding/bond2**
9 ☐	Configure NTP server address on SDM Server A and Server B	• Use the TPD menu front-end to configure server clock synchronization with NTP: **# su – platcfg** navigate through Main Menu -> Network Configuration -> NTP -> Edit : ntpserver1: **NTP_IP**  • Navigate the menus back to the main menu and Exit • Force the system to synchronize now: **#service ntpd stop** **#service ntpdate start** **#service ntpd start** - Force the system to update immediately the real-time clock managed by the BIOS

		# hwclock --systohc
		• Verify system time is now good, and the NTP “offset” value is now small
		# ntpq -c lpeers
		Example output:
		`remote refid st t when poll reach delay offset jitter`
		`==============================================================================`
		`*ntpserver1 .GPS. 1 u 66 128 377 0.203 0.006 0.005`
		`ntpserver2 .INIT. 16 u 783 1024 0 0.000 0.000 0.000`
		• The offset with the reference clock shoul be close to 0.000.

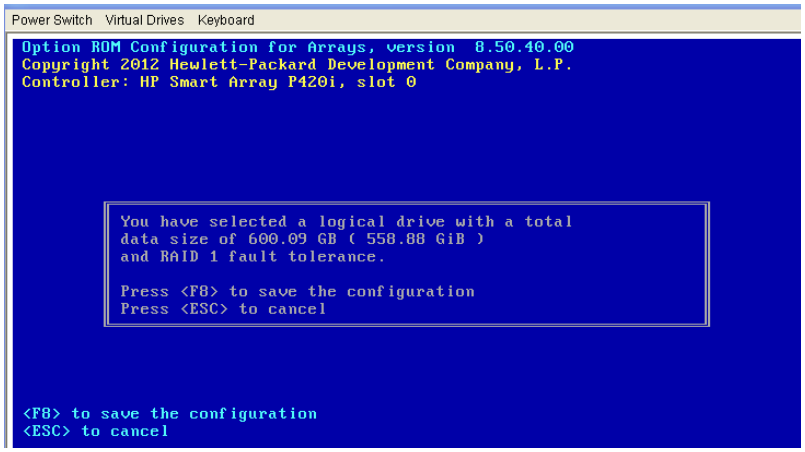
10 ☐	Create the required SDM RAID1 setup on SDM server A and server B	**Create the RAID configuration from Raid controller menu (only for configuration with additional hard drives).** The RAID 1+0 configuration can be performed by following steps below : - using the iLO, connect to the virtual console of the system - use the "CAD" icon on the virtual console to generate a Ctrl-Alt-Del sequence, or the power button to generate a power-down/power-up sequence - when the message "Press any key to see Option ROM messages", press any key - when the message **"Press F8 for Slot 0 controller"** appears, press F8 - Select "View Logical Drive" to confirm a drive is configured, then Escape to return to the main menu - You have to use the raid controller menu to configure the hardware RAID the following way: **Disk Bay 3&4 : RAID1** **Disk Bay 5&6 RAID1** **Disk Bay 7&8 RAID1** - Select the "Create Logical Drive" entry and use the TAB key and the space bar to deselect all the disks except the four first one:



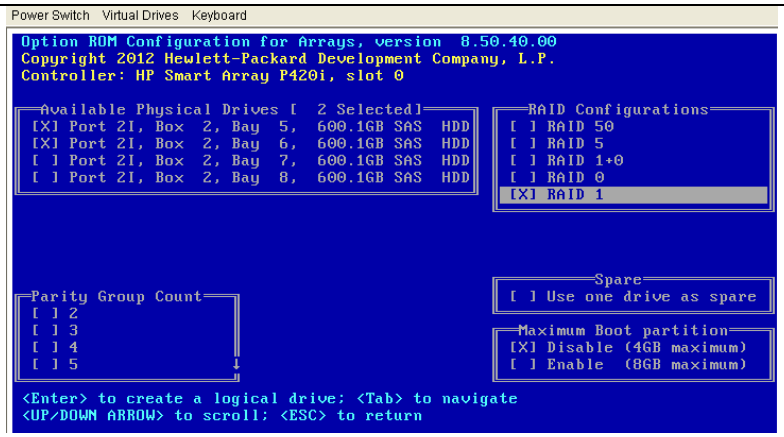
Press enter to confirm you choice, the display should look like :

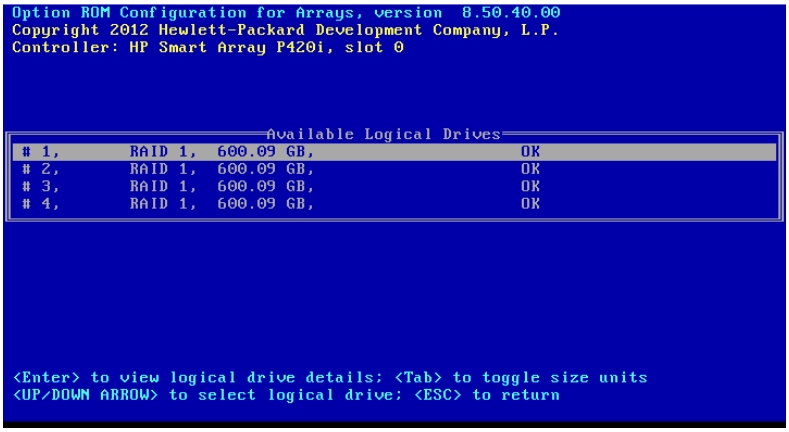


Press F8 to save the configuration:



- Repeat the process for the other four drives:

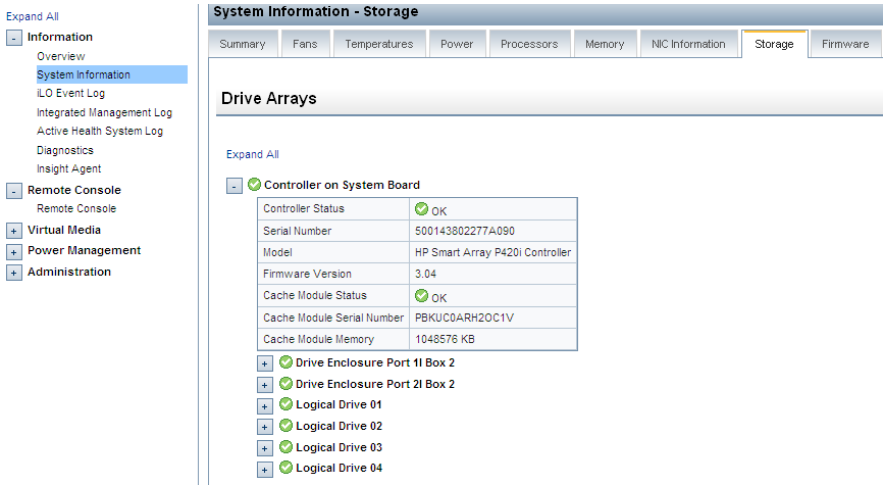


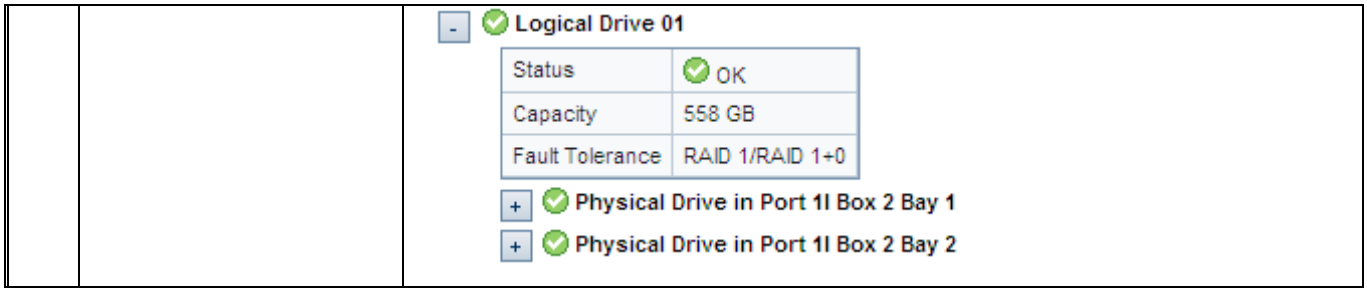


- Once the RAID1 configuration is completed, press <ESC> to exit and let the blade boot normally..

11 ☐ Verify the Drive Array configuration from the iLO4.

Check the 4 logical drives From the iLO4 menu *Information => System Information* under storage :



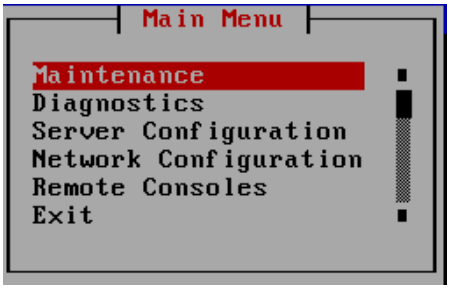
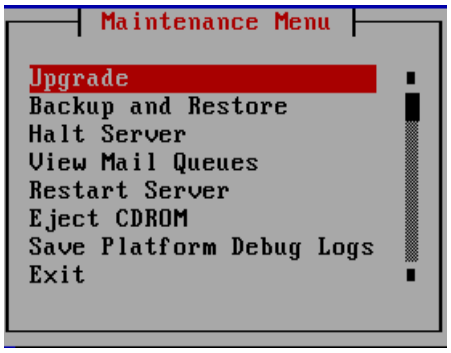

Logical Drive 01
Status
OK
Capacity
558 GB
Fault Tolerance
RAID 1/RAID 1+0
Physical Drive in Port 1I Box 2 Bay 1
Physical Drive in Port 1I Box 2 Bay 2

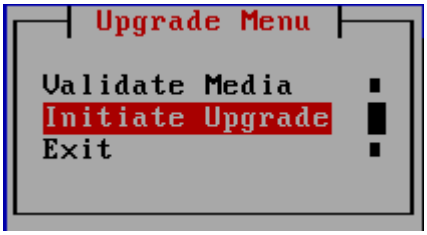
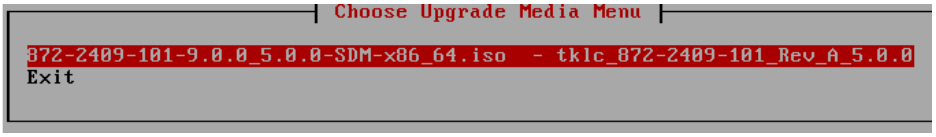
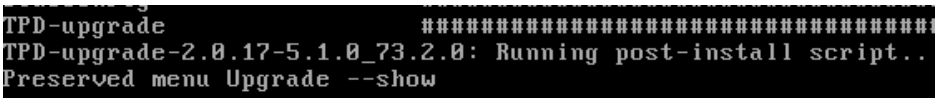
5.0 BASIC INSTALLATION AND CONFIGURATION OF SDM SOFTWARE

S T E P #	Steps to be completed.	This installation must be repeated for each DL380 server planned to be part of the SDM/TPD configuration.It describes how to install edit the configuration files required by SDM platform nd how to install the SDM iso. **Needed material:** - SDM release 9.0 software image 872-2409-101-9.0.0_5.0.0-SDM-x86_64.iso Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.
1 ☐	Edit blue file on SDM server A and SDM server B	Using SSH or the virtual console of each DL380 server, login to the root account, and create the file /etc/sysconfig/blue with the following contents: Example of Blue File in SDM Server A SYSTEMTYPE=RACKMOUNT SITENAME=CSLAB_RMS2 SHELFID=1 **SLOTID=1** PRIVATEINTERFACE=bond0 PUBLICINTERFACE=bond2 SINGLEFRAGMENTDB=1 Example of Blue File in SDM Server B SYSTEMTYPE=RACKMOUNT SITENAME=CSLAB_RMS2 SHELFID=1 **SLOTID=2** PRIVATEINTERFACE=bond0 PUBLICINTERFACE=bond2 SINGLEFRAGMENTDB=1 For Geo-Redundancy Only Note: If geo-redundancy is used, file /etc/sysconfig/blue must contain two extra lines: For DL380 servers in **SDM1 (site 1)**, the two extra lines in file /etc/sysconfig/blue should be: SITESUFFIX=_1 SITESUFFIXREMOTE=_2 For DL380 servers in **SDM2 (site 2)**, the two extra lines in file /etc/sysconfig/blue should be:

		SITESUFFIX=_2 SITESUFFIXREMOTE=_1 Make sure that there are no space characters left in the /etc/sysconfig/blue file and that SRPDOMAIN value is the same in all servers that belong to a same SDM system.

2 ☐	Add the sdmvlans.conf file on SDM Server A :	• Prepare a sdm-vlans.conf file for the SDM installation.
		• Using SSH or the virtual console of each DL380 server, login to the root account.
		• Copy the prepared sdm-vlans.conf file to:
		/etc/sysconfig/sdm-vlans.conf
		.
		Example of sdm-vlans.conf file:
		`169.254.0.0 16 255.255.0.0 0.0.0.0 bond0 1 main`
		`10.240.230.32 28 255.255.254.0 10.240.230.33 bond1 1 xmi`
		`10.240.230.48 28 255.255.254.0 10.240.230.49 bond2 1 xsi1`
		
		Column 1: Network address
		Column 2: subnet size
		Column 3: subnet mask
		Column 4: Gateway address
		Column 5: Interface
		Column 6: Vlan Id
		Column 7: Network name [one of main, SDMxmi, SDMxsi1, SDMxsi2]
		
		• If geo-redundancy is used, file /etc/sysconfig/sdm-vlans-conf must contain two extra lines:
		`GEO _NET GEO_MASK_SIZE GEO_MASK GEO_GATEWAY bond1 GEO_Subnet_ID xmi`
		`GEO_2_SDM_VIP/32 PREFSRC GEO_1_SDM_VIP`
		
		`GEO_NET GEO_MASK_SIZE GEO_MASK GEO_GATEWAY bond1 GEO_Subnet_ID main`
		`GEO_2_SDM_VIP/32 PREFSRC GEO_1_SDM_VIP`
		
		Note : A sample of sdm-vlans.conf can be found under **/blue/etc/sdm-vlans.conf.sample** and used for preparing the sdm-vlans.conf file for this installation.
		Note: For installations that do not use VLANs, this file is still REQUIRED. The value 1 is used in column 6 (…. **1** main).
		Note : You may need to add extra lines in the sdm-vlans.conf file depending on the remote subnets connected to the SPR node (eg . MPEs in different site),please refer to [TK6] TR006928

		The instuctions commented in sdm-vlans.conf.sample file must be followed .Special characters such as underscore "_" are not supported in Column 7.
3 ☐	Transfer the SDM software to the servers SDM1 and SDM2 Server A and Server B	• Using the network or some media (ex. A USB key), transport the SDM software to directory /var/TKLC/upgrade on the Blade Server, then verify the results (the exact file name shown here may vary depending on version): **# ls /var/TKLC/upgrade/**
4 ☐	Validate the SDM SPR iso media	• Check that the SDM Blue iso is not corrupted using platcfg menu : **Maintenance → Upgrade → Validate Media** The iso media should not report any error : Validating cdrom... ## ## ## ## ## ## UMVT Validate Utility v2.2.1, (c)Oracle June 2010 Validating /var/TKLC/upgrade/872-2409-101-9.0.0_5.0.0-SDM-x86_64.iso Date&Time: 2012-11-07 18:20:59 Volume ID: tklc_872-2409-101_Rev_A_5.0.0 Part Number: 872-2409-101_Rev_A Version: 5.0.0 Disc Label: SDM Disc description: SDM The media validation is complete, the result is: PASS CDROM is Valid PRESS ANY KEY TO RETURN TO THE PLATCFG MENU.
5 ☐	Install SDM software on SDM1 and SDM2 server A and server B :	**# su – platcfg** **Maintenance → Upgrade → Initiate Upgrade**  

		 Select the SDM SPR 9.0.0 iso in order to initiate the installation.  If the TPD requires to be upgraded,the script will perform a TPD upgrade.  The server will reboot automatically.
6	Verify the Software version and the platform version	Once the reboot and installation are completed,run the following command Verify TPD version **# getPlatRev** **5.1.0-73.3.0** • Verify the software version **# BlueVersion** **** Blueslice version: 9.0.0_5.0.0**
7 ☐	Execute the system controller command (only on SDM1 and SDM2 server A)	**Only do the steps if this DL380 server is the very first member of a new SDM installation, and no SDM-specific database exists yet (otherwise, this step may cause SDM data loss!). For all other DL380 servers in the SDM installation, skip to the next page:** Run the configurecontroller command on the first server of each cluster **# configurecontroller.sh –blue** and watch output messages for eventual errors. • > Processing Parameters configurecontroller.sh: Creating /blue/etc/SystemModel_Loaded.xml... configurecontroller.sh: /blue/etc/SystemModel.xml configurecontroller.sh: /blue/etc/default/BnGlobalAudit.xml

		• configurecontroller.sh: /blue/etc/default/DrmDefaultConfig.xml • configurecontroller.sh: /blue/etc/default/PMJobDefs.xml • configurecontroller.sh: /blue/etc/default/PMThresholdDefs.xml • configurecontroller.sh: /blue/etc/SystemModel_RACKMOUNT.xml • …… • configurecontroller.sh: /blue/etc/appcfg/SystemModel_hss.xml • configurecontroller.sh: /blue/etc/appcfg/SystemModel_lte.xml • configurecontroller.sh: /blue/etc/appcfg/SystemModel_ras.xml • configurecontroller.sh: /blue/etc/appcfg/SystemModel_sip.xml • configurecontroller.sh: /blue/etc/SystemModelNoFragment.xml • configurecontroller.sh: Loading the system model... • configurecontroller.sh: /blue/etc/SystemModel_Loaded.xml • > Blueslice Information Schema provisioned successfully • Shutting down SelfReliant 7500 • .....stopped • mysqlblued: Stopping MySQL..... stopped.

6.0 PERFORM SSH KEYS EXCHANGE

Procedure 5. SDM ssh configuration.

S T E P #	Steps to be completed.	This procedure is aimed at performing the ssh keys exchanges between all the SDM blades belonging to the system.It has to be executed on active system controller blade on each site. **Needed material:** - SDM release 9.0 software installed on each Server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.
1 ☐	Edit the sdm-ssh.conf files:	the files to be edited are called ***sdm-ssh.conf*** and must be placed in **/etc/sysconfig/ on Active system controller blades in** each site An example of this file is located under /etc/sysconfig sdm-ssh.conf.sample - Prepare two ***sdm-ssh.conf*** files for each SDM site. - **sdm-ssh-tool** script should be under /blue/bin directory **# vim /etc/sysconfig/sdm-ssh.conf**  sdm-ssh.conf.sample **EXAMPLE FOR SITE 1 :** LOCAL-GROUP CSLAB-SPR1 **# list below all the blades used in SDM SPR site 1 (private IPs and public IPs)** MEMBER CSLAB-SPR1-BLADE1 IP-LIST 169.254.1.1 10.15.63.141 MEMBER CSLAB-SPR1-BLADE2 IP-LIST 169.254.1.2 10.15.63.142 **# list below all local VIPs in cluster in site 1 that require ssh functions** **(private VIP is always 169.254.1.20 and GEO VIP1,OAMP VIP,PROVSIONNING VIP)** LOCAL-VIPS 169.254.1.20 **10.15.63.139 10.15.63.134 10.15.63.135** **# list below the remote site name and the loal and remote Geo VIPS** REMOTE-GROUP CSLAB-SPR2 VIPS 10.15.63.140 USE-LOCAL-VIPS **10.15.63.139** **EXAMPLE FOR SITE 2 :**

		LOCAL-GROUP CSLAB-SPR**2** **# list below all the blades used in SDM SPR site 2 (private IPs and public IPs)** MEMBER CSLAB-SPR2-BLADE1 IP-LIST 169.254.1.1 10.15.63.143 MEMBER CSLAB-SPR2-BLADE2 IP-LIST 169.254.1.2 10.15.63.144 **# list below all local VIPs in cluster in site 2 that require ssh functions (private VIP 169.254.1.20 and GEO VIP, OAMP VIP,PROVSIONNING VIP)** LOCAL-VIPS 169.254.1.20 **10.15.63.140 10.15.63.136 10.15.63.137** **# list below the remote site name and the loal and remote Geo VIPS** REMOTE-GROUP CSLAB-SPR**1** VIPS **10.15.63.139** USE-LOCAL-VIPS **10.15.63.140**
2 ☐	Generate brand new ssh keys on both sites:	Run the following command on each **Active** system controller (blade where the configurecontroller command has been executed in step 19) on **both sites SDM1 and SDM2** to generate ssh keys for all the blades of the SDM system : **# /blue/bin/sdm-ssh-tool --reset** SDM SSH tool version 1.09 82810 Erasing all key-related files in /etc/ssh ... Erasing all key-related files in /root/.ssh ... Restarting SSH server (causes host key regeneration) ... Stopping sshd: [OK] Generating SSH1 RSA host key: [OK] Generating SSH2 RSA host key: [OK] Generating SSH2 DSA host key: [OK] Starting sshd: [OK] Generating new SSH user key ...
3 ☐	Mount manually the Geo VIPs on each site:	On SDM1 site : ***# setvip.sh bond1 Geo_VIP1 Netmask*** */blue/bin/setvip.sh: Adding IP Geo_VIP1 to interface bond1* */blue/bin/setvip.sh: Updating ARP caches on subnet XXMI_SUBNET/xMASK* On SDM2 site: ***# setvip.sh bond1 Geo_VIP2 Netmask*** Verify that the Geo VIPs are properly mounted to the active system controller blades on each site :

		Note: The Geo VIP has to be mounted on the Geo interface (could be OAM or XSI). **#ip -f inet addr** 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue inet 127.0.0.1/8 scope host lo 5: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue inet 192.168.1.245/24 brd 192.168.1.255 scope global bond0 9: bond0.142@bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue inet 10.15.63.141/27 brd 10.15.63.159 scope global bond0.142 **inet 10.15.63.139/32 brd 10.15.63.139 scope global bond0.142** 10: bond0.146@bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue inet 169.254.1.1/16 brd 169.254.255.255 scope global bond0.146 inet 169.254.254.2/32 brd 169.254.254.2 scope global bond0.146
4 ☐	Exchange the ssh keys	Run the following command on each **Active** system controller on **both** sites SDM1 and SDM2 to perform automatically the ssh key exchanges : **# /blue/bin/sdm-ssh-tool –fix --wizard-override** SDM SSH tool version 1.09 82810 WARNING *** Emergency wizard override requested *** Starting SDM SSH local fixes... NOTICE: Cannot read file /root/.ssh/authorized_keys Cannot read /root/.ssh/authorized_keys, re-creating the file **NOTICE: File /root/.ssh/known_hosts not readable, re-creating it** **NOTICE: Resetting correct line for host 127.0.0.1 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host localhost in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 169.254.1.1 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 10.15.63.143 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 169.254.1.2 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 10.15.63.144 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 169.254.1.20 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 10.15.63.140 in /root/.ssh/known_hosts** Generating temporary SSH user key...OK REMOTE group SLAB-SPR1 may be reachable through 1 VIP(s) Starting fix attempt for REMOTE group SLAB-SPR1... Trying to ping remote grp at 10.15.63.139 ... Successful at 100% Do you wish to attempt connecting to REMOTE grp SLAB-SPR1? (Y/n): Y

		Do you wish to attempt connecting to REMOTE grp CSLAB-SPR1? (Y/n): • **Enter "Y" when the script resquests confirmation to connect to remote SPR site.** *** Will attempt to reach REMOTE group CSLAB-SPR2 at 10.15.63.139 **Type the root password shared by all nodes in REMOTE grp CSLAB-SPR1:** • **Enter root password when the script requests it to connect to the remote site** **Type the root password shared by all nodes in REMOTE grp SLAB-SPR1:** **Testing basic SSH to REMOTE group SLAB-SPR1...** **Setting up SSH connection... Connection OK** **NOTICE: Resetting correct line for host 10.15.63.139 in /root/.ssh/known_hosts** **Trying to get root user pub key from REMOTE SLAB-SPR1 ... OK** **ERROR: Actual REMOTE group name in public key does not match our configuration** **Building SDM SSH fix network drop...** **Type the root password shared by all nodes in system CSLAB-SPR2:** • **Enter root password when the script requests it to connect to the local blades** **NOTICE: Resetting correct line for host 127.0.0.1 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host localhost in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 169.254.1.1 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 10.15.63.143 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 169.254.1.2 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 10.15.63.144 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 169.254.1.20 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 10.15.63.140 in /root/.ssh/known_hosts** **NOTICE: Resetting correct line for host 10.15.63.139 in /root/.ssh/known_hosts**

		• Verify that ssh works properly between all blades private IPs,localhost hand between Geo VIPs
5 ☐	Verify that ssh keys are properly exchanged	Run the following command on each **Active** system controller on **both** sites to perform automtically the ssh key verification step : **# /blue/bin/sdm-ssh-tool --check** DM SSH tool version 1.09 82810 Starting SDM SSH check... Starting SDM SSH local checks... NOTICE: No line in /root/.ssh/authorized_keys for REMOTE group SLAB-SPR1 1 notice/warning(s) found during local check. Starting SDM SSH local network checks... **Type the root password shared by all nodes in system CSLAB-SPR2:** • **Enter root password when the script requests it to connect to the local blades** If all the verificaton steps are passed the following lines should be observed : **For Active system controller :** **0 notice/warning(s) found during local network check.** **0 notice/warning(s) found during local network check** **0 notice/warning(s) checking remote group** **For each local blades :** **0 notice/warning(s) found during local check.** **0 notice/warning(s) found during signature and REMOTE group check.**
6 ☐	Clear the GEO VIPs on both sites:	On each SPR cluster on the Active system controller clear the local Geo VIP manually.

		On SDM1 site : ***# clearvip.sh Geo_VIP1*** */blue/bin/clearvip.sh: Removing route to default for VIP 10.15.63.139 in table sdmoam1* */blue/bin/clearvip.sh: Removing VIP 10.15.63.139 from bond0.142* On SDM2 site : ***# clearvip.sh Geo_VIP2*** /blue/bin/clearvip.sh: Deleting preferred source routes for VIP 10.15.63.140 /blue/bin/clearvip.sh: Removing route to default for VIP 10.15.63.140 in table xmi /blue/bin/clearvip.sh: Removing VIP 10.15.63.140 from bond0.142 Verify that the Geo VIPs are properly cleared from the active system controller blades on each site : **#ip -f inet addr**

7.0 CONFIGURE SPR APPLICATION

Procedure 6. SDM disks configuration and SPR application installation

S T E P #	Steps to be completed.	This proceduremust be repeated for each DL380 server planned to be part of the SDM/TPD configuration.It describes how to configure the SDM partitions and the SDM application (Load SPR schema,configure HSS,RESTful interface,licenses,SNMP) **Needed material:** - SDM subscribers license (.lkey file) - HSS diameter licenses for each HSS Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. **IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.**
1 ☐	Create SDM Partitions *(only if additional disks are used)*	If the DL380 server where you are installing SDM has additionnal 8 hard drives, launch the automated disk configuration script. **Otherwise, skip to next step.** **# perl /blue/etc/create_SDMdiskconfig.pl** Succesful completion should report: Fri Jun 17 15:10:05 2011 successfully created and mounted SDM volumes: SDMBin, SDMDb, SDMLog. Fri Jun 17 15:10:05 2011 system is ready to run SDM. Fri Jun 17 15:10:05 2011 /root/create_SDMdiskconfig.pl Done **OK.** • Check the Physical and logical volunes : **#lvdisplay --map | grep -e "Physical volume" -e "LV Name"** LV Name /dev/vgroot/plat_root Physical volume /dev/cciss/c0d0p2 LV Name /dev/vgroot/plat_var Physical volume /dev/cciss/c0d0p2 LV Name /dev/vgroot/plat_usr Physical volume /dev/cciss/c0d0p2 LV Name /dev/vgroot/plat_tmp Physical volume /dev/cciss/c0d0p2 LV Name /dev/vgroot/plat_var_tklc Physical volume /dev/cciss/c0d0p2 LV Name /dev/vgroot/SDM Physical volume /dev/cciss/c0d0p2 LV Name **/dev/vgroot/SDMBin** Physical volume /dev/cciss/c0d1p1 LV Name /dev/vgroot/SDMDb Physical volume /dev/cciss/c0d2p1 LV Name /dev/vgroot/SDMLog

Physical volume /dev/cciss/c0d3p1

- Check that the SDM partitions have been created

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root
                      992M  374M  568M  40% /
/dev/mapper/vgroot-plat_tmp
                      992M   34M  908M   4% /tmp
/dev/mapper/vgroot-plat_usr
                      3.9G  2.9G  820M  79% /usr
/dev/mapper/vgroot-plat_var
                      992M   78M  863M   9% /var
/dev/mapper/vgroot-plat_var_tklc
                      3.9G  1.3G  2.5G  34% /var/TKLC
/dev/cciss/c0d0p1     251M   23M  216M  10% /boot
tmpfs                  32G     0   32G   0% /dev/shm
/dev/mapper/vgroot-SDM
                      540G  814M  511G   1% /var/TKLC/SDM
/dev/mapper/vgroot-SDMBin
                      551G  206M  522G   1% /var/TKLC/SDMBin
/dev/mapper/vgroot-SDMDb
                      551G  326M  522G   1% /var/TKLC/SDMDb
/dev/mapper/vgroot-SDMLog
                      551G   21G  502G   4% /var/TKLC/SDMLog
```

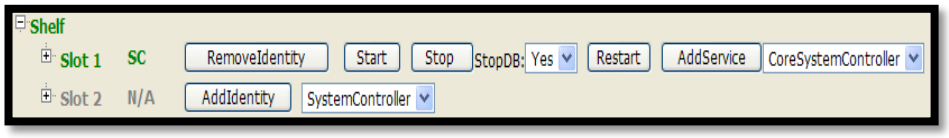
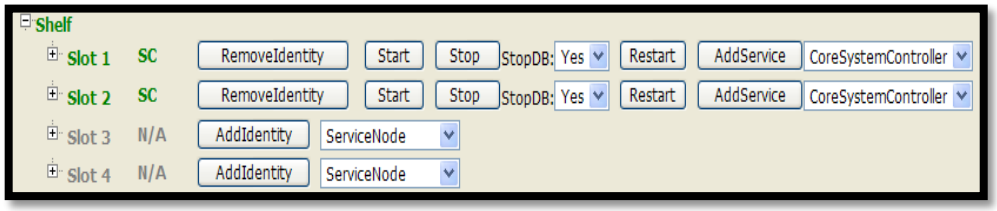
Filesystem	Size	Physical volume	LV name	partition	Soft linked to
/dev/mapper/vgroot-SDM	540GB	c0d0p2	/dev/vgroot/SDM	/var/TKLC/SDM	/blue /export
/dev/mapper/vgroot-SDMBin	551GB	c0d1p1	/dev/vgroot/SDMBin	/var/TKLC/SDMBin	/blue/var/dbbin
/dev/mapper/vgroot-SDMDb	551GB	c0d2p1	/dev/vgroot/SDMDb	/var/TKLC/SDMDb	/blue/var/db
/dev/mapper/vgroot-SDMLog	551GB	c0d3p1	/dev/vgroot/SDMLog	/var/TKLC/SDMLog	/blue/var/dblog

2 ☐ Start the blue Services on SDM server A on SDM1 site

Run the 1st start the first SPR blade :

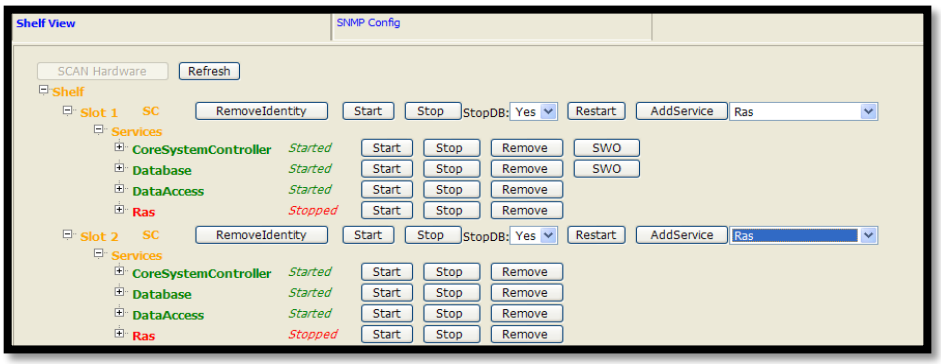
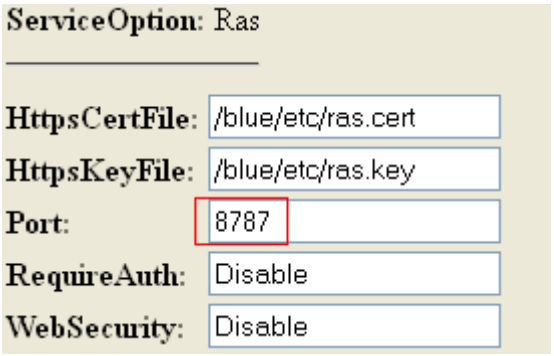
 # service blue start

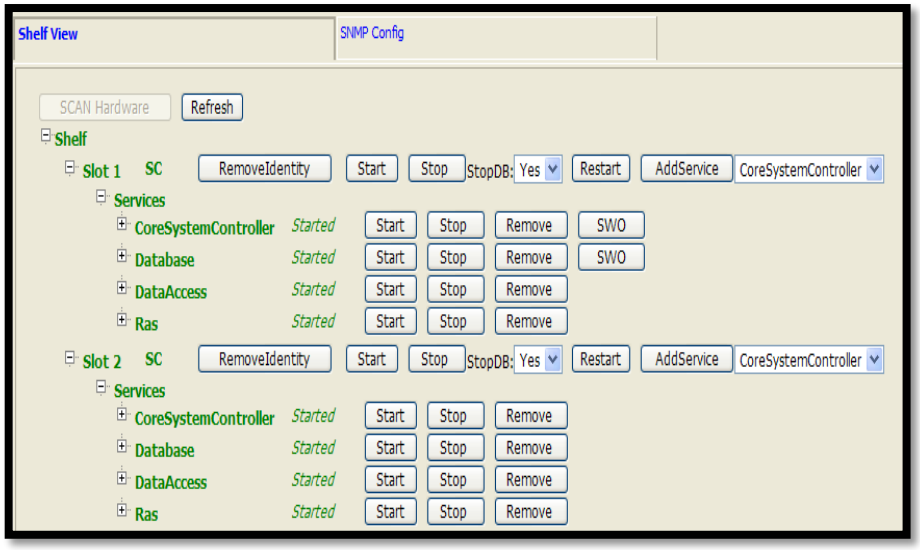
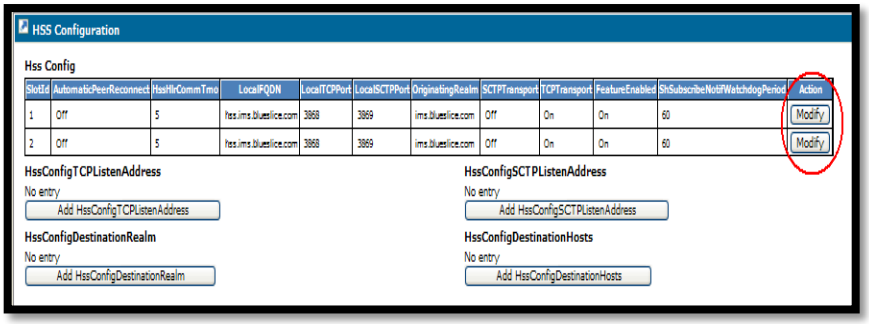
- Starting backend database
- mysqlblued: Starting MySQL..... started.
- Starting tungsten replicator
- **No active SC found**
- blue: Starting.....
- OampManager: Started (3237)
- OampEventMgr: Started (3457)
- OampPerformanceManager: Started (3553)
- WebCI: Started (3654)
- Snmp: Port 161 has been used by other application. Blusesnmpd start up failed!

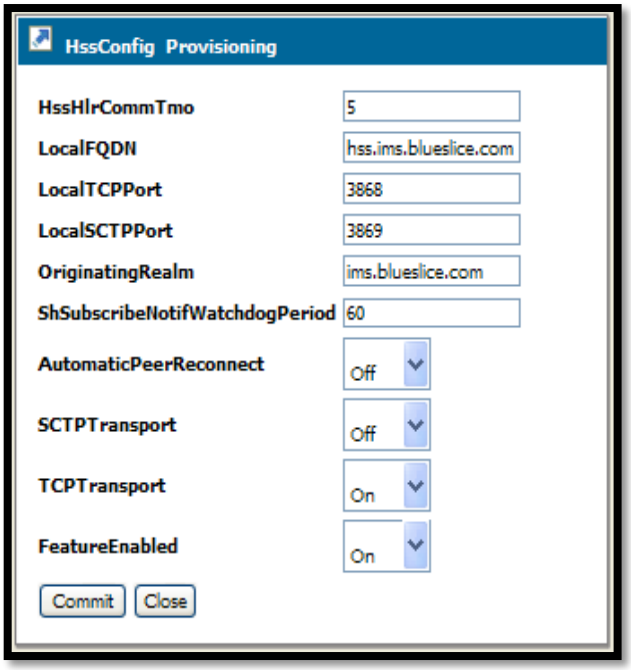
		• **CoreSystemController: Started** • Database: Started • blue: Waiting for system to initialize... Done • blue: Waiting local database activation... Done • DataAccessServer: Started (6759) • XmlDataServer: Started (6922) • blue: Started Verify that the SDM web management interface (WebCI) is now active, by connecting from a web browser located on some other system on the customer XMI to URL http://XMI_SDM_VIP_IP:8080 using the IP address of the 1st DL380 server on which SDM is installed. • Verify the value of SDM_TPD_UNIQUE_SLOT_ID_X that is configured in file /etc/sysconfig/blue on that system**.** • In the **WebCI interface**, define the Slot ID of that system as a System Controller **Oracle SDM™ → System - ID:→ Shelf View** 
3 ☐	Add the System Controller Identity to others SDM Blade Server	For each additional server in this clsuter: • verify the value of SDM_UNIQUE_SLOT_ID that will be configured in file **/etc/sysconfig/blue** on that systemin the WebCI interface, • define the Slot ID of that system as a core sytem controller. 
4 ☐	Load SPR Schema on 1st SDM Blade Server	Connect to the active system controller blade that has just been started in step 26 • Connect to BlueCli **# BlueCli -u admin** • Execute the Following command to load the Policy Schema :

		1 :> Schema[]: **2 :Schema[]> ProcessFile() Dir = /blue/etc; File = Policy.xml** Done!
5 ☐	Start the Application on the Standby SDM Blade Server	For all subsequent blade servers manually do the first start of the SDM services: **# service blue start** **CoreSystemController: Started** Database: Started blue: Waiting for system to initialize... Done blue: Waiting local database activation... Done On SPR2 standby and execute the following command : #blue/usr/local/tungsten-replicator/tungsten-replicator/bin/trepctl services Processing services command... NAME VALUE **appliedLastSeqno: 3362878736** **appliedLatency : 1.013** role : slave **serviceName : blue__1_1** serviceType : local started : true state : ONLINE NAME VALUE ---- ----- **appliedLastSeqno: 107355** **appliedLatency : 0.794** role : master **serviceName : blue__1_2** serviceType : local started : true state : ONLINE Finished services command... The output result should give * : • ***"local Master"*** service ***blue__x_y*** with an acceptable latency less than1 second. • Verify that there is a ***"local Slave"*** service ***blue__x_z*** with an acceptable latency less than1 second. * "***x"*** refers to the site_suffix of SPR2 site installed, ***"y"*** refers to the slotId of active system controller ..."***z"*** refers to the slotId of standby system controller
6 ☐	Add the OAM and provisioning VIPs	• Connect to the BlueCli **# BlueCli –u admin** • Execute the following commands to add the OAM Virtual IP:

		:System[ ]:Shelf[ShelfId = 1] **AddVip() Netmask = XMI_MASK; Vip = XMI_SDM_VIP ; VipType = 1** Now you can connect to the Webci using the OAM Vip : **http:// XMI_SDM_VIP:8080** **Note: WebCi is listening on port 8080** • Execute the following commands to add the Provisioning Virtual IP: **AddVip() Netmask = XMI_MASK; Vip = PROV_SDM_VIP ; VipType = 3**
7 ☐	Install SDM/SPR License on 1st SDM blade.	• Transfer the license file to 1st SDM blade Server under **/export** • Execute the following commands : **# LicenseInsataller –f /var/TKLC/upgrade/*license-file.lkey*** > Installing the license... ********** *** The license key was successfully installed. *** ********** • Verify that the command is successfully executed and and connect to the Webci to check the system name and License :  **License Info** Issuer Name : Copyright 2009, Blueslice Networks, Inc. All Rights Reserved Issued Date : April/02/2009 Customer Name : TEKELEC-01 Total Subscribers HLR : 5000000 Active Subscribers HLR : 5000000 Total Subscribers SIP (AOR) : 5000000 Registration Bindings SIP : 5000000 Total Subscribers HSS : 5000000 Total Subscribers SLF : 5000000 Total Subscribers AAA : 5000000 AAA Max TPS (per blade) : 500 Total Subscribers SPR : 5000000
8 ☐	Add Ras services on each SPR server	If **RESTful** interface is used for provisionning , add the Ras service on the WebCi for both servers and start the service.

		Otherwise, skip to next step. • In the **WebCI interface**, define the Slot ID of that system as a System Controller **Oracle SDM™ → System - ID:→ Shelf View** • Got to the far right pull down and select the Ras service • Select Add Service on **Slot 1** and **Slot 2** 
9	Configure the Ras options	If **RESTful** interface is used for provisionning , add the Ras service on the WebCI for both servers and start the service. **Otherwise, skip to next step.** Configure the Ras options from **Oracle SDM™ → Service Management:→ Option**  1) Specify the certificates and key files for HTTPS (HttpsCertFile, HttpsKeyFile) 2) Enable HTTPS if required ; WebSecurity: Enable 3) Enable HTTP Authentication if required 4) Change the Ras port if reauired (default 8787) <u>Update the changes:</u>  <u>Start Ras services :</u> • Start the Ras Service on **Slot 1**

		• Wait a minute then select the refresh button • Start the Ras Service on **Slot 2** • Wait a minute then select the refresh button 
10 ☐	Add HSS services manually	• Add the HSS service using the same proccess as the Ras - Configure the **Hss Config** parameters such as **LocalFQDN,localTCPPort,OriginatingRealm, etc** **Oracle SDM™ → HSS→ HSS Configuration**  • Modify

<table>
<tr><td></td><td></td><td> 
</td></tr>
<tr><td>11</td><td>Configure the RESTful interface parameters.</td><td>Configure the RESTful interface and provisionning parameters :
HSS → HSS System Features→ HssSPRConfig
<table>
<tr><td>ForceReadOnMaster</td><td>Off</td></tr>
<tr><td>MNCCodeLength</td><td>2</td></tr>
<tr><td>RESTCDataSectionEscaped</td><td>Off</td></tr>
<tr><td>RESTIgnoreUnknownBody</td><td>Off</td></tr>
<tr><td>RESTIgnoreContentType</td><td>Off</td></tr>
<tr><td>RESTIgnoreOpaqueDataMismatchName</td><td>Off</td></tr>
<tr><td>RESTIgnoreAcceptHeader</td><td>Off</td></tr>
<tr><td>RESTTransactionCommitTimeout</td><td>100</td></tr>
<tr><td>RESTTransactionMaxRequest</td><td>10</td></tr>
<tr><td>HttpDisablePlus</td><td>On</td></tr>
<tr><td>HttpDoubleEncoding</td><td>Off</td></tr>
<tr><td>HttpEscaping</td><td>On</td></tr>
<tr><td>HttpChunkedTimeout</td><td>0</td></tr>
</table>
Modify

Please refer to PR220558 for more details on these SPR parameters.</td></tr>
<tr><td>12
</td><td>Add HP Diameter License on each server running HSS service</td><td>Edit the script Add_codewords.sh by adding the codewords provided by the Project Manager at the end of the file after “add’:

restart_hpoc
sleep 5
$OCLICOAM add coderword#0_to_be_added_here
$OCLICOAM add coderword#1_to_be_added_here
$OCLICOAM save</td></tr>
</table>

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

Transfer Add_codewords.sh under /export to the SDM blades running Hss service
Execute the script on SDM blades running Hss service:

Add_codewords.sh

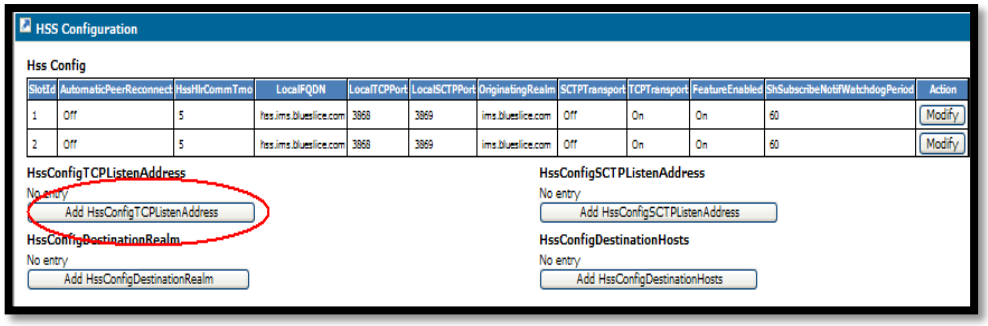
bash /export/Add_codewords.sh

*** Stopping HPOC licenses infrastructure.
Shutting down HP OpenCall License Server daemon:
[OK]
Shutting down gmfprovd: [OK
*** Starting HPOC licenses infrastructure.
Starting gmfprovd: [OK]
Starting HP OpenCall License Server daemon:
[OK]
OCLICOAM-S-ADDCODEWORD, Codeword successfully added
OCLICOAM-S-ADDCODEWORD, Codeword successfully added
OCLICOAM-S-SAVE, Codeword successfully saved
*** Installed HPOC codewords:
0 coderword#0
1 coderword#1

Verify the HSS capacity on SDM server A and server B
/opt/OC/bin//oclicoam show max all

Expected output :

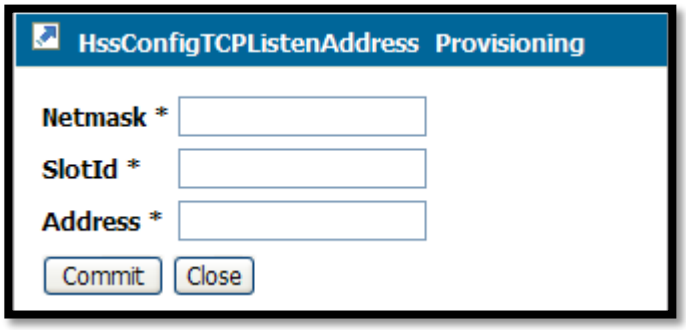
Feature ate Amount Version ExpiryD
------- ------- ---------- ----------
OcDiamAuth 1 1.3 Unlimited
OcDiamTps 800 1.3 Un limited
</td>
</tr>
<tr>
<td>13</td>
<td>Configure Sh interface</td>
<td>Configure the Sh Signaling IPs on 1st and 2nd SDM Blade Server (XSI-1 IP adresses and eventually XSI-2)
Oracle SDM™ → HSS→ HSS Configuration</td>
</tr>
</table>



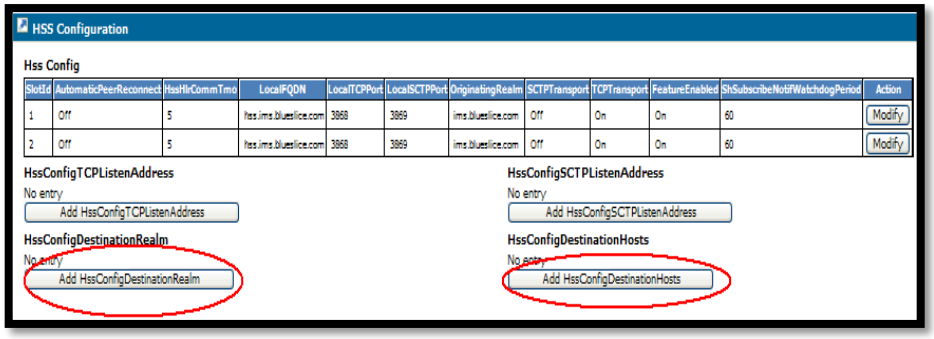
Netmask: **XSI-1_MASK**

SlotId: **SDM_UNIQUE_SLOT_ID**

Address: **XSI-1_SDM_VIP**



- Configure the Destination diameter peer parameters (realm,hosts)



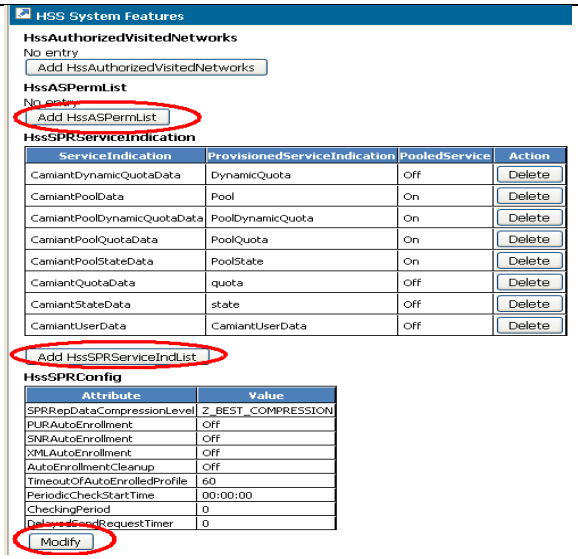
HssConfigDestinationRealm: To provision the domains only from which the connections are accepted.

Example: **LocalRealm = ims.blueslice.com**

HssConfigDestinationHosts: To provision the hosts only from which the connections are accepted.

Example: **LocalFQDN = hss.ims.blueslice.com**

14	Configure HSS system features	



Configure the HssSystemOptions:

Turn On/Off the SPR functionality's Auto-Enrollment feature. This feature can be useful in the cases where the subscriber profiles are initially stored outside of the SPR.

PURAutoEnrollment = **ON/OFF**

SNRAutoEnrollment = **ON/OFF**

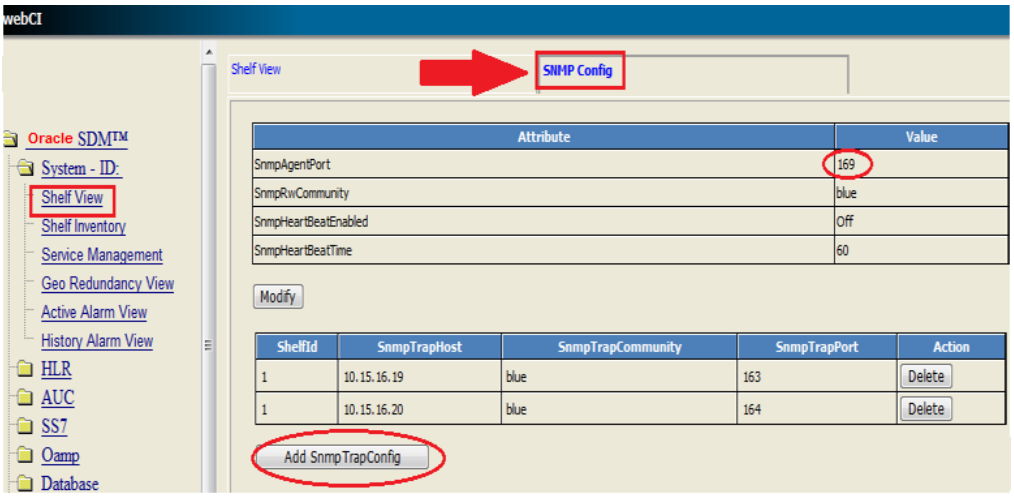
AutoEnrollmentCleanup = **ON/OFF**

Set the compression level the IMS-HSS must use when storing the service data in the HssSPRRepositoryData.

SPRRepDataCompressionLevel= Z_BEST_**COMPRESSION**

15 Configure the SNMP on 1st and 2nd SPR cluster

Oracle SDM™ → System - ID: → Shelf View → SNMP Config

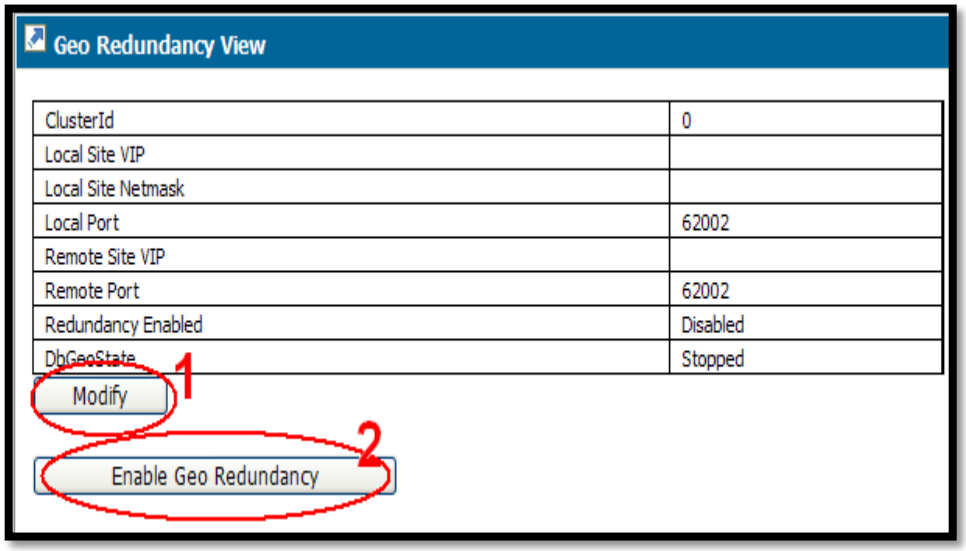


- Change SnmpAgentPort to 163

		• Add Snmp Traps with customer information • Restart SNMP Service **# bluesnmpd restart** • Verify SNMP is runing • **# ps -ef | grep snmp** root 6012 1 0 Aug29 ? 00:20:09 /usr/sbin/snmpd -Lsd -Lf /dev/null -p /var/run/snmpd.pid -a root 27873 1 2 15:39 ? 00:00:00 bluesnmpd -f -Lo -c /blue/etc/snmpd.conf root 27905 27136 0 15:39 pts/0 00:00:00 grep snmp

8.0 GEO REDUNDANCY CONFIGURATION

Procedure 7. GEO Redundancy configuration

STEP #	Steps to be completed.	This procedure describes the steps to configure and enable the Geographical redundancy for SDM/SPR 9.0 system **Needed material:** Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.
1 ☐	Exchange the SSH keys for GEO VIP SDM1 (SITE1)	**Note: ICMP flow needed between sites for GEO-redundancy** **Note: The VIP used for Geo redundancy must be different from OAM and Provisionning VIP** • This part has been executed in **procedure 4** • If ssh keys were not exchanged perform procedure 4 now
2 ☐	Configure Geo Redundancy parameters on SDM1 (site 1):	Configure the GEO Redundancy From Webci On the 1st SDM Blade Server: **Oracle SDM™ → System - ID:→ Geo Redundancy View** Local Site VIP= Local Site Netmask= Remote Site VIP= 
3 ☐	Enable Geo Redundancy	At this step the Redundancy Enabled should be *Enabled* At this step the DbGeoState should be *Stopped* Redundancy Enabled **Enabled** DbGeoState **Stopped**

<table>
<tr>
<td>4
☐</td>
<td>Restart SDM1 (site 1) services to enable Geo Redundancy</td>
<td>
The service must be restarted to Take effect:

Stop Services on 2nd SDM Blade Server (standby System Controller):

service blue stop

• Restart Services on 1st SDM Blade Server (Active System Controller):

service blue restart

Note: When the first system controller blade on SDM site#1 is restarted with geo-redundancy enabled, the server will first try to connect to the SDM2 to determine if it should go reference or replica. The system will try for 5 minutes to connect to the peer site#2, as site 2 is not started, it will go to the reference State

The System will be in this State during approximately 5 minutes :

blue: Waiting for system to initialize....

Then the active system controller starts as a reference database.

At this point Geo Redundancy is enabled only on SDM1 alarm 2207 should be raised by DpController due to remote site unreachable.

293 2207 Critical Geographic reference site running unprotected Mon Jun 6 18:26:03 2011

• On Webci in SDM1,Verify the current Geo Redundancy configuration :

Under System ID => Geo Redundancy View :

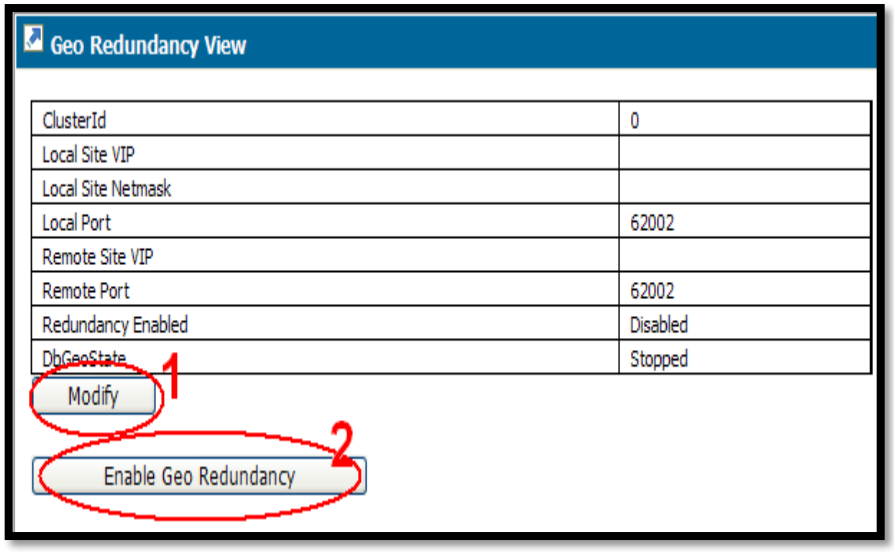
<table>
<tr><td>ClusterId</td><td>0</td></tr>
<tr><td>Local Site VIP</td><td>10.240.230.46</td></tr>
<tr><td>Local Site Netmask</td><td>255.255.255.0</td></tr>
<tr><td>Local Port</td><td>62002</td></tr>
<tr><td>Remote Site VIP</td><td>10.240.241.10</td></tr>
<tr><td>Remote Port</td><td>62002</td></tr>
<tr><td>Redundancy Enabled</td><td>Enabled</td></tr>
<tr><td>DbGeoState</td><td>Reference</td></tr>
</table>

The DbGeoState should be “reference” , “Enabled”

• If SDM2 is planned to be configured later,the procedure is completed for SDM1
</td>
</tr>
<tr>
<td>5
☐</td>
<td>Configure Geo Redundancy parameters on SDM2 (site 2)</td>
<td>
Configure the GEO Redundancy From Webci

On the 1st SDM Blade Server:

Oracle SDM™ → System - ID:→ Geo Redundancy View
Local Site VIP=
Local Site Netmask=
Remote Site VIP=
</td>
</tr>
</table>

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


Enable Geo Redundancy

At this step the Redundancy Enabled should be Enabled
At this step the DbGeoState should be Stopped

<table>
<tr><td>Redundancy Enabled</td><td>Enabled</td></tr>
<tr><td>DbGeoState</td><td>Stopped</td></tr>
</table>
</td>
</tr>
<tr>
<td>6
☐</td>
<td>Restart SDM services to enable Geo Redundancy</td>
<td>
Stop Services on 2nd SDM Blade Server (standby System Controller):

service blue stop

Restart Services on 1st SDM Blade Server (Active System Controller):

service blue restart

The System will be synchronize with SDM1 :

blue: Waiting for system to initialize....

Then server A SDM2 (active system controller) starts as a replica database
On Webci in SDM2,Verify the current Geo Redundancy configuration :

Under System – ID => Geo Redundancy View :

<table>
<tr><td>ClusterId</td><td>0</td></tr>
<tr><td>Local Site VIP</td><td>10.240.241.10</td></tr>
<tr><td>Local Site Netmask</td><td>255.255.255.0</td></tr>
<tr><td>Local Port</td><td>62002</td></tr>
<tr><td>Remote Site VIP</td><td>10.240.230.46</td></tr>
<tr><td>Remote Port</td><td>62002</td></tr>
<tr><td>Redundancy Enabled</td><td>Enabled</td></tr>
<tr><td>DbGeoState</td><td>Replica</td></tr>
</table>

The DbGeoState should be “Replica”,”Enabled”
</td>
</tr>
</table>

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

On Webci in SDM1,Verify the current Geo Redundancy configuration :
Under System – ID => Geo Redundancy View :

<table>
<tr><td>ClusterId</td><td>0</td></tr>
<tr><td>Local Site VIP</td><td>10.240.230.46</td></tr>
<tr><td>Local Site Netmask</td><td>255.255.255.0</td></tr>
<tr><td>Local Port</td><td>62002</td></tr>
<tr><td>Remote Site VIP</td><td>10.240.241.10</td></tr>
<tr><td>Remote Port</td><td>62002</td></tr>
<tr><td>Redundancy Enabled</td><td>Enabled</td></tr>
<tr><td>DbGeoState</td><td>ReferenceProtected</td></tr>
</table>
The DbGeoState should be changed to “referenceProtected”
</td>
</tr>
<tr>
<td>7
☐</td>
<td>Start Services standby System Controller servers on SDM1 and SDM2 sites</td>
<td>

Start Services on 1st and 2nd SDM Blade Server (active and standby System Controller):
service blue start
At this point the Geo Redundancy configuration is completed
Verify the Dtabase replication status for Geo redundancy :

/blue/usr/local/tungsten-replicator/tungsten-replicator/bin/trepctl services

Processing services command...
NAME VALUE
---- -----
appliedLastSeqno: 1126485905
appliedLatency : 0.169
role : master
serviceName : blue__2_1
serviceType : local
started : true
state : ONLINE

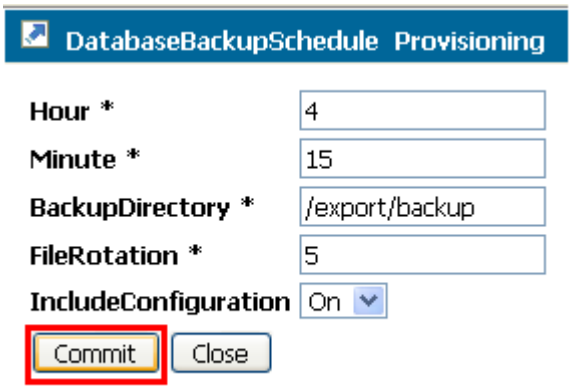
NAME VALUE
---- -----
appliedLastSeqno: 3217536761
appliedLatency : 0.868
role : slave
serviceName : blue__1_1
serviceType : remote
started : true
state : ONLINE
NAME VALUE
---- -----
---- -----

Verify that there is a “local Master” service blue__x_y with an acceptable latency less than1 second.
Verify that there is a “local slave” service blue__t_y with an acceptable latency less than1 second.

* ”x” refers to the site_suffix of the first SPR site installed,
”t” refers to the site_suffix of second SPR site installed,
”y” refers to the slotId of active system controller
...”z” refers to the slotId of standby system controller
</td>
</tr>
</table>

9.0 SDM SPR DATABASE BACKUP SCHEDULE AND NETBACKUP CLIENT CONFIGURATION

Procedure 8. SPR Database Backup schedule and NetBackup Client configurattion

S T E P #	Steps to be completed.	This procedure describes the steps to configure the database backup schedule on SDM/SPR system and a NetBackup client. **Needed material:** • Application server platform installation has been completed. • Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured. • NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server. • For Network requirements refer to [4] TR007093 Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.
1 ☐	Activate the backup schedule on SDM	Connect to the WebCi under ***Database => Backup/Restore/DRM*** : Select *'Add DatabaseBackupSchedule'* under **DatabaseBackupSchedule** menu :  **Hour :** Hour of day for scheduled backups **Minute:** Minute of day for scheduled backups **BackupDirectory** : Directory for scheduled backup **FileRotation :** Number of backups to keep on the system Activate the Datbase backup schedule by clicking on Activate button :  Verify that the DatbaseBackupSchedule is properly configured and activated in WebCi :

DatabaseBackupSchedule

Attribute	Value
Hour	4
Minute	15
DatabaseId	Subscriber Database
BackupDirectory	/export
IncludeConfiguration	On
FileRotation	5
IsActivated	On

Disable | Modify | Delete

2 ☐ Enable the push NETBACKUP Client from platcfg

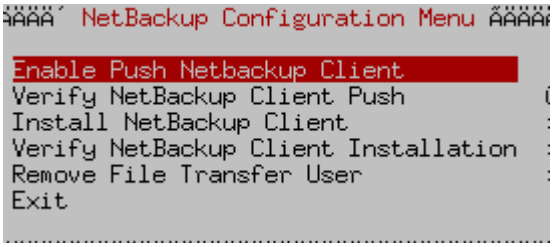
For more details on how to configure NetBackup client refer to [TK7] section 3.14.5 **Application NetBackup Client Procedures.**

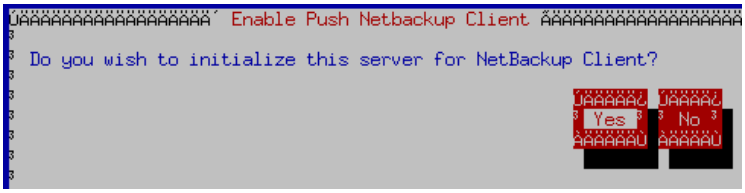
Depending on the Interconnect strategy ,additionnal lines might be added to sdm-vlans.conf file.Refer to Appendix C for interconnect strategy methods with Netbackup server on DL380.Dedicated bandwidth is recommended.

Connect to platcfg menu :

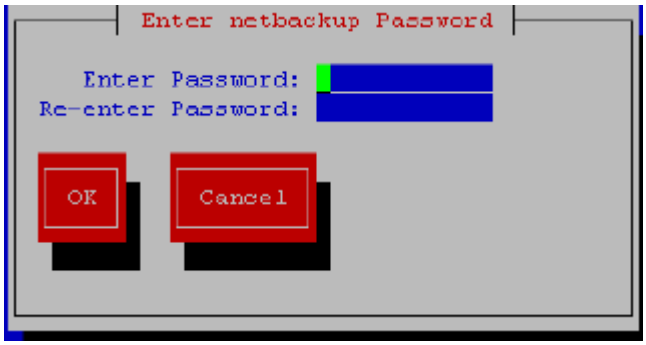
 # su – platcfg

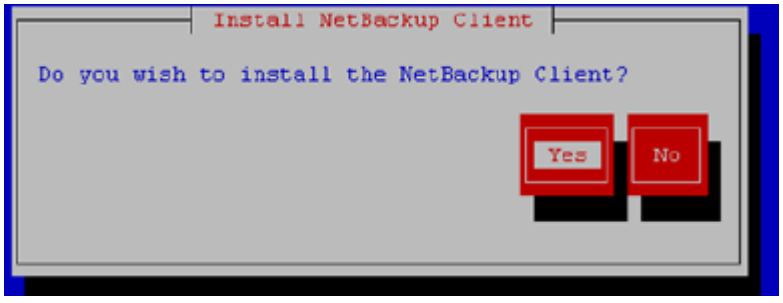
NetBackup Configuration → Enable Push Netbackup Client → Yes

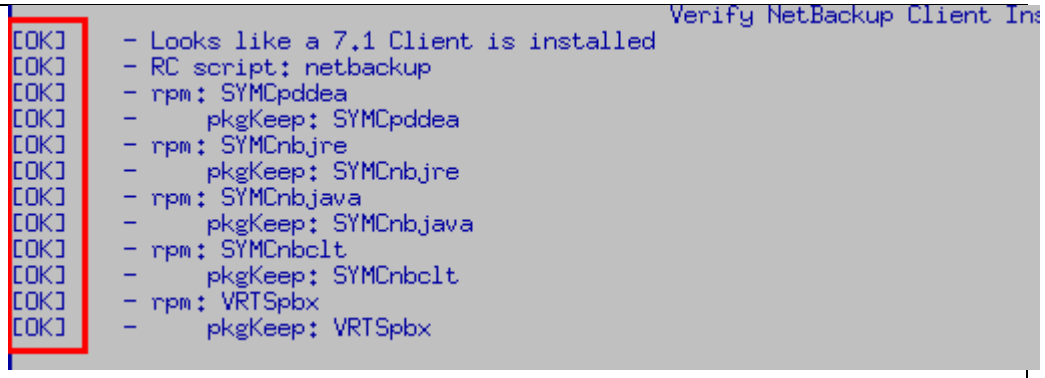




- Enter NetBackup password and select OK :



3 ☐	Verify NetBackup Client software push is enabled and update SPR hosts file	**NetBackup Configuration → Verify NetBackup Client Push** Verify NetBackup Client Envi [OK] - User acct set up: netbackup [OK] - User netbackup shell set up: /usr/bin/rssh [OK] - Home directory: /home/rssh/home/netbackup [OK] - Tmp directory: /home/rssh/tmp [OK] - Tmp directory perms: 1777 • Update the application hosts file with NetBackup server infos **# cd /etc** **# rcstool co hosts** **# echo "***NetBackup_server_IP Netbackup_server_hostname***" >> hosts** **# rcstool ci hosts**
4 ☐	Install the Netbackup Client Application	**Note:** The NetBackup server is not an application asset. Access to the NetBackup server, and location path of the NetBackup Client software is under the control of the customer. The steps to configure the NetBackup server to push the NetBackup Client software to the application server can be found in [TK1].**These steps are not within the scope of this document** **Note:** The backup server is supported by the customer, and the backup utility software provider. If this procedural STEP, executed at the backup utility server, fails to execute successfully, STOP and contact the Customer Care Center of the backup and restore utility software provider that is being used at this site. • Once the client software has been pushed by sftp from the Server do the following steps : **# su – platcfg** **NetBackup Configuration → Install Netbackup Client**  • Verify the NetBackup Client Installation from ***platcfg*** menu: **NetBackup Configuration → Verify Netbackup Client Installation**

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


Verify that the NetBackup server hostname has been added to /usr/openv/netbackup/bp.conf file
# cat /usr/openv/netbackup/bp.conf
SERVER = Netbackup_server_hostname
CLIENT_NAME = 10.15.58.210
CONNECT_OPTIONS = localhost 1 0 2

</td>
</tr>
<tr>
<td>5 ☐</td>
<td>Activate the client on the server side from bpadm</td>
<td>

Activate the client on the server side from bpadm:

Select the desired Policy :

Policy: TKLCDaily
Clients: vmback1 en20001b07 ...
Schedules: Daily
Output Destination: SCREEN

Policy Management
----
a) Add Policy...
m) Modify Policy Attributes...
d) Delete Policy
s) Schedule Management...
c) Client List Management...
f) File List Management...
t) Catalog Backup Disaster Recovery...

b) Browse Policies Forward
r) Browse Policies Reverse
e) Enter Policy
l) List/Display Policies
o) Output Destination (SCREEN or FILE)
h) Help
q) Quit Menu

ENTER CHOICE: b

Add The SPR OAMP VIP to the client List by selecting

Client List management → Add Clients → Linux-IA64, RedHat2.6
</td>
</tr>
</table>

		Enter clients of Linux-IA64, RedHat2.6 type: (blank line to end) Enter Client Name: ***SPR_hostname*** • Display the Policy to verify the clients **List/Display Policy** : **Linux-IA64 RedHat2.6 *SPR1_hostname*** **Linux-IA64 RedHat2.6 *SPR2_hostname*** • Verify NetBackup connectivity from the server **# get_remote_host_version** XMI_SDM_VIP **7.1** **Note:** The important directories/files from SPR that should be included in the Backup are : Include: /export/backup /etc/sysconfig /boot/grub /var/log /blue/var/log /var/TKLC/log

APPENDIX A: SDM-VLANS.CONF.SAMPLE

```
# File /etc/sysconfig/sdm-vlans.conf.sample
# ----------------------------------------
# Sample config file for "SDM Advanced Routing for Virtual IPs"
#
# File /etc/sysconfig/sdm-vlans.conf is used by SDM to modify
# IP routing to support Virtual IPs (VIPs). IP routing is modified
# when a VIP is activated and when it is deactivated. This also applies
# when a VIP moves from a blade to another (i.e. VIP deactivation
# on blade X, VIP activation on blade Y).
#
# Note that this file has no involvement with IPs declared
# statically (activated by Linux during normal system startup).
# This means that basic IP routing (static default routes, etc.)
# must STILL be configured sufficiently for SDM blades to communicate
# correctly when a blade has no virtual IPs active.
#
#
# IMPORTANT: In order to use SDM Advanced Routing for Virtual IPs,
#       copy this file to /etc/sysconfig/sdm-vlans.conf on
#       the Active System Controller, and configure the subnets
#       according to the customer's network requirements.
#
#       If the file /etc/sysconfig/sdm-vlans.conf is very large,
#       activation/deactivation time for Virtual IPs may increase.
#       You may want to remove most of these comments from
#       the actual running file /etc/sysconfig/sdm-vlans.conf  ,
#       and leave these comments in /etc/sysconfig/sdm-vlans.conf.sample
#
# IMPORTANT: In the following description, a "prefix" is
#       an IP subnet base followed by a subnet size,
#       for example 10.1.2.0/24
#
# IMPORTANT: The old Linux commands "netstat -rn" and "ifconfig -a"
#       are often misleading.
#
#       Use the command "ip -f inet addr" to see the list of
#       IPv4 addresses on the system.
#       Use the command "ip rule list" to see the list
#       of policy-routing rules, and the command
#       "ip route list table <name>" to see the routing
#       entries associated with each table referenced
#       by the policy-routing rules.
#
#
# This file is accessed by SDM software on a blade in three scenarios:
# ---------------------------------------------------------------------
# 1. When SDM software starts (i.e. "service blue start"),
#   if a blade is NOT the Active System Controller,
#   the file is copied FROM the Active System Controller
#   into our local /etc/sysconfig/sdm-vlans.conf.
#
# 2. When a Virtual IP is activated on the blade.
#
```

```
# 3. When a Virtual IP is deactivated on the blade.
#
#
# How to safely modify the VIP routing environment while SDM is running:
# ------------------------------------------------------------------
#
# 1. Use SDM software (WebCI, BlueCLI, etc.) to deactivate the Virtual IPs
#    that are in subnets for which you need to change the routing
#    configuration.
#
# 2. On all SDM blades in the SDM group, verify with "ip -f inet addr"
#    that the Virtual IPs for the subnets to be modified are no longer active.
#
# 3. Modify /etc/sysconfig/sdm-vlans.conf for the appropriate subnets.
#    Make sure the resulting file is identical on all SDM blades
#    in the SDM group.
#
# 4. Reactivate the affected Virtual IPs in SDM software.
#
#
# Syntax of this file:
# --------------------
# a) Each line that begins with "#" is a comment.
#
# b) Blank lines are ignored.
#
# c) Any other line should contain the following fields
#    separated by white space:
#
#    <subnet_base> <subnet_size> <subnet_mask> <gateway_ip> <nw_intf> <vlan_id> <table_name>
[<options>]
#
#       where <options>, if present, may take one of the following forms:
#
#          <prefix>
#          PREFSRC <src_ip>
#          <prefix> PREFSRC <src_ip>
#
# d) Rules on configuration lines:
#
#    i. If a VIP matches more than one variant of <subnet_base>/<subnet_size>,
#       only the most-specific matches are used (the matches with the
#       largest size. In other words, if you have lines like this:
#
#       10.1.0.0 16 255.255.0.0   <rest of line 1 config>
#       10.1.0.0 16 255.255.0.0   <rest of line 2 config>
#       10.1.2.0 24 255.255.255.0 <rest of line 3 config>
#       10.1.2.0 24 255.255.255.0 <rest of line 4 config>
#
#       when VIP 10.1.1.3 activates or deactivates, only lines 1 and 2 apply
#       when VIP 10.1.2.3 activates or deactivates, only liens 3 and 4 apply
#
#    ii. a config line is only accepted by SDM is <subnet_size> has the
#        exact same meaning as <subnet_mask>, i.e.
#
#        a line that begins with "172.30.1.0 24 255.255.255.0   ..."   is OK
```

```
#       a line that begins with "172.30.1.0 25 255.255.255.128 ...    is OK
#       but
#       a line that begins with "172.30.1.0 25 255.255.255.0 ..."  is rejected
#
#    iii. if a subnet is private and non-routable,
#         specify <gateway_ip> to be 0.0.0.0 and leave <options> blank
#
#    iv. if a subnet must be placed on an interface which has no VLANs,
#       or on the "untagged" VLAN of an interface, specify <vlan_id> to be 1
#
#    v. If <table_name> is "main", this route is chosen based on the
#       destination IP address of a packet emitted by the SDM blade,
#       regardless of what the source IP address is.
#
#       If <table_name> is not "main", this route is chosen FIRST based
#       on the source IP address of a packet emitted by the SDM blade.
#       Then, <dest_prefix> needs to be matched for the route to be chosen.
#
#    vi. <options> can be one of the following variants:
#
#       ""  this is a default route,
#                                   i.e. <dest_prefix> = 0.0.0.0/0
#
#       <dest_prefix>   route applies only to this destination prefix
#
#       PREFSRC <src_ip>   this is a default route, and use <src_ip>
#                       as the source IP address in this case
#
#       <dest_prefix> PREFSRC <src_ip>  route applies only to thi destination prefix, and use <src_ip> as
the source IP address
#
#
# Sample lines that show what can be configured:
# -----------------------------------------------
#
# a) When the SDM internal OAM VIP activates
#    (SDM requires that the internal OAM subnet must be
#     169.254.0.0/16), SDM configures it on bond0 Vlan 24 ,
#    and this subnet is non-routable.
#
#   169.254.0.0  16  255.255.0.0  0.0.0.0  bond0  24  main
#
# b) When a VIP in subnet 10.1.2.0/26 (util1) activates,
#    configure it on eth01 (no VLAN). Any packets
#    emitted with a source IP address in 10.1.2.0/26
#    is sent to gateway 10.1.2.1 regardless of the destination IP.
#
#   10.1.2.0  26  255.255.255.192  10.1.2.1  eth01  1  util1
#
# c) When a VIP in subnet 10.12.13.0/24 (sigtran1) activates,
#    configure it on bond0 Vlan 103. Route packets based
#    on the destination IP. Packets to 192.168.10.0/24 go to
#    10.12.13.1, packets to 192.168.20.0/24 go to 10.12.13.2.
#    Nothing is specified for other subnets (default static routing
#    will be used)
#
```

```
#   10.12.13.0  24  255.255.255.0  10.12.13.1  bond0  103  sigtran1  192.168.10.0/24
#   10.12.13.0  24  255.255.255.0  10.12.13.2  bond0  103  sigtran1  192.168.20.0/24
#
# d) Geo-Redundancy and COS provisioning example:
#
#    Subnet 10.35.47.0/24 (sdmadm1) is on interface bond0 Vlan 114,
#    the subnet can contain two local VIPs:
#         local Geo-Redundancy VIP is 10.35.47.10,
#         and COS provisioning VIP is 10.35.47.11.
#    The remote Geo-redundancy VIP is 172.30.24.113.
#
#    Any packets using a source IP in 10.35.47.0/24 are sent to
#    gateway 10.35.47.1. If they are sent to the distant Geo-redundancy VIP,
#    the preferred source IP is the local Geo-redundancy VIP.
#
#    For packets where the source IP does not match any other
#    source-based routing rules (we reach routing table "main"),
#    if the destination IP is the distant geo-redundant VIP,
#    set the preferred source IP to the local Geo-redundancy VIP.
```

APPENDIX B: SDM-SSH.CONF SAMPLE

```
# File /etc/sysconfig/sdm-ssh.conf.sample
# "$Id: sdm-ssh.conf.sample 82563 2011-08-22 14:57:55Z mchatel $"
#
# To be able to use "sdm-ssh-tool", you must make a MODIFIED
# copy of this file in /etc/sysconfig/sdm-ssh.conf ,
# adapted to the specific SDM network configuration being used.
#
# Terminology: SDM member - a single running installation of Linux with SDM
#                       (usually on a multi-CPU, multi-core machine)
#
#            SDM group  - a collection of SDM members intended to run
#                       synchronized with the same Active System Controller
#
#            SDM remote group - a distant SDM group with which we need
#                           to run Geo-Redundancy traffic
#
#
# 1- Define the local SDM "group with its logical name.
#    This logical name is to be used in the identifier part of the root
#    account DSA key pair and is shared by all members in the group.
#
#    In this lab example, the name is intended to convey the meaning
#    "C-class #1, this SDM group contains blades 1,3,5,6"
#
LOCAL-GROUP CSLAB-SPR1
  #
  # Define all members of the group. The member logical names
  # are only used in SDM-SSH-TOOL diagnostic messages
  # and do not need to match the Linux host names.
  #
  # For each member, list the static IP addresses that may be
  # destination IPs for SSH connections initiated by other members.
  #
  # Typically, for each member, the static private IP and the
  # static public IP on the SDM OAM network should be listed.
  #
  MEMBER CSLAB-SPR1-BLADE1 IP-LIST 169.254.1.1 10.15.63.141
  MEMBER CSLAB-SPR1-BLADE2 IP-LIST 169.254.1.2 10.15.63.142
  #MEMBER CSLAB-SPR2-BLADE1 IP-LIST169.254.1.1 10.15.63.145
  #MEMBER CSLAB-SPR2-BLADE2 IP-LIST 169.254.1.2 10.15.63.146
  #
  # Define the list of virtual IPs of the group that may be
  # destination IPs for SSH connections initiated by any member.
  #
  # Virtual IPs that will NEVER be used as destination IPs
  # in SSH connections do not need to be listed here.
  #
  LOCAL-VIPS 169.254.1.20 10.15.63.139
  #
#
# There may be zero or more SDM remote groups with which we needi
# to run Geo-Redundancy traffic. If SDM-SSH-TOOL is also installed
# and used on the remote group, the remote-group name defined here
```

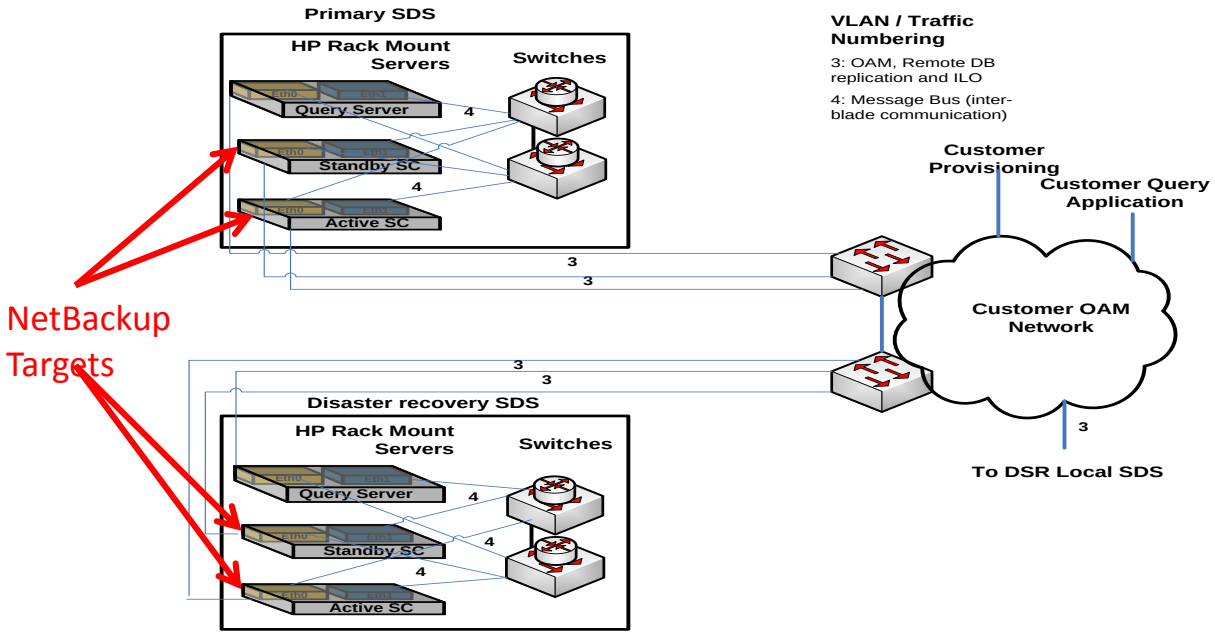
```
# should match the LOCAL-GROUP name used on the remote group.
#
# One or more remote VIPs may be associated with the remote group.
# These are VIPs that must be reachable as SSH destinations from any
# member in our local group.
#
# Typically, because of firewall or routing restrictions, there may
# be only one local SDM member that is able to reach the remote group,
# usually the member that has the local geo-redundancy Virtual IP active.
# So the remote group specification allows configuring one or more
# Virtual IP for the remote group, and one or more local VIPs.
# SDM-SSH-TOOL can only attempt to check & fix remote group keys if it
# is started on a member that has one or more of these local VIPs active !
#
REMOTE-GROUP CSLAB-SPR2 VIPS 10.15.63.140 USE-LOCAL-VIPS 10.15.63.139
```

APPENDIX C: NETBACKUP INTERCONNECT STRATEGY

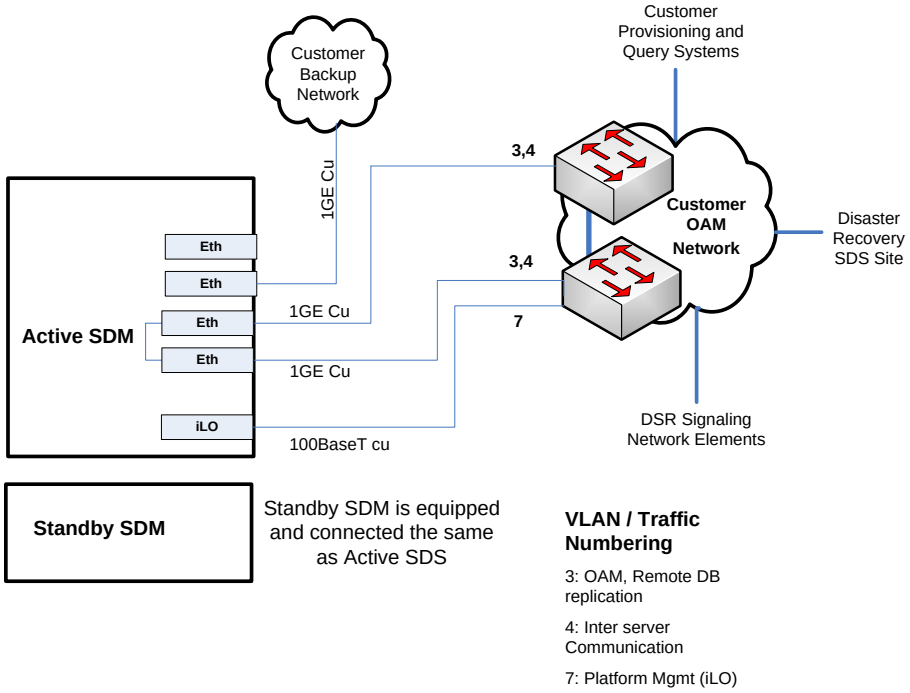
By default, backup activities would share the same bandwidth as XMI and XSI activities (method 1). This can lead to serious performance degradation during the backup time windows, while transfer of backups take place over the network.

As a result, it is recommended to guarantee bandwidth separation between applications and backups by setting up distinct network paths for them.

For DL380 rackmount servers, one Gigabit Ethernet port on each node should be reserved for connection to the customer's NetBackup infrastructure. If it is decided that not all SDM nodes will be NetBackup clients, only the NetBackup client nodes require the backup Gigabit Ethernet connection. (method 2) XSI-2 interface can be used for this purpose.



Method 1 Example Deployment - SDM uses XMI for NetBackup in Rackmount configuration



Method 2 Example Deployment - SDM utilizes dedicated uplink for NetBackup in Rackmount configuration (XSI-2 recommended)