Oracle® Communications Subscriber Data Management

Installing SPR 9.0 on HP C-Class G8

Release 9.0

E63815-01

November 2012

ORACLE®

Oracle Communications Subscriber Data Management, Installing SPR 9.0 on HP C-Class G8, Release 9.0

Copyright ©2010, 2012 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

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

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

Table of Contents

***1.0* PURPOSE AND SCOPE 5**
1.1 Acronyms 5
1.2 References 6
1.3 High Level networking Description 7
1.4 Installation Restrictions 8
1.5 Installation Prerequisites 8
1.5.1 Networks List in C-CLASS server 9
1.5.2 XMI configuration 9
1.5.3 Traffic or XSI-1 configuration 10
1.5.4 Traffic or XSI-2 configuration 10
1.5.5 NTP 10
1.5.6 Adding Private Network 10
1.5.7 Adding Additional Parameters 11
1.6 Authentication 11
1.7 Basic installation of TPD 11
1.8 Acquiring Firmware 11
1.9 C-CLASS Configuration with additional drives 12

2.0 INSTALLATION (AND NETWORKING) IN A C-CLASS ENVIRONMENT 13
2.1 PM&C Installation 13
2.2 Configure Aggregation Switch 13
2.3 Complete the PM&C Installation 13
2.4 HP C-7000 Enclosure Configuration 14

3.0 LOADING SDM AND TPD SOFTWARE IMAGES ONTO THE PM&C 15

4.0 UPDATE APPLICATION BLADE FIRMWARE 17

5.0 ADJUST POWER MANAGEMENT AND INSTALL TPD VIA PM&C 23

6.0 BASIC POST INSTALL CONFIGURATION OF TPD ON EACH C-CLASS SERVER 33

7.0 BASIC INSTALLATION AND CONFIGURATION OF SDM SOFTWARE 40

8.0 PERFORM SSH KEYS EXCHANGE 45

9.0 CONFIGURE SPR APPLICATION 51

10.0 GEO REDUNDANCY CONFIGURATION 63

11.0 SDM SPR DATABASE BACKUP SCHEDULE AND NETBACKUP CLIENT CONFIGURATION 67

APPENDIX A: SDM-VLANS.CONF.SAMPLE 72

APPENDIX B: SDM-SSH.CONF SAMPLE 76

APPENDIX C: NETBACKUP INTERCONNECT STRATEGY 78

List of Figures

Figure 1: SPR on C-CLASS Connectivity figure 7

List of Tables

Table 1: Acronyms 5
Table 2: References 6
Table 3: Network List in C-CLASS server 9
Table 4: XMI configuration 9
Table 5: XSI-1 configuration 10
Table 6: XSI-2 configuration 10
Table 7: IMI configuration 10
Table 8: C-CLASS HW configuration types 12

1.0 PURPOSE AND SCOPE

The purpose of this document is to document the installation of SDM/SPR 9.0.0 software on the TPD 5.2.1 Linux environment, on HP C-CLASS G8 hardware.
This document describes only methods utilized and procedures executed to configure the 9.0 SDM/SPR application.

It is assumed that:

- The hardware installation and network cabling were executed beforehand.
- The HP c-Class system to be used with Policy 9.x and SDM 9.0 has been setup following WI006729 [TK8]Policy 9.x Software Installation Guide procedures 1 to 13 listed below :

- Procedure 1. Install TVOE 2.0 on Management Server (DL360/DL380)
- Procedure 2. Upgrade DL360/380 Server Firmware
- Procedure 3. TVOE/Management Server Network Configuration
- Procedure 4. Install PM&C Application
- Procedure 5. Configure PM&C Access to Cisco 4948 Aggregation switch
- Procedure 6: Verify and Update Switch IOS
- Procedure 7: Configure Aggregation Switches with netConfig
- Procedure 8. Configure the PM&C Application
- Procedure 9. Configure OA IP Address (via front panel display)
- Procedure 10. Performing the Initial OA Configuration (OA Configuration Wizard)
- Procedure 11. Adding the Cabinet and Enclosure to PM&C
- Procedure 12: Configuring Enclosure Bay iLO Passwords
- Procedure 13. Configure HP 6120XG Switch Pair(s) using NetConfig

This document is intended for Oracle Tekelec field personnel who need to install SDM software on C-CLASS 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 C-CLASS 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	
[TK7]	PF006110	SDM 9.0 Product Functional Specification	
[TK8]	WI006729	Policy 9.x Software Installation Guide	

Table 2: References

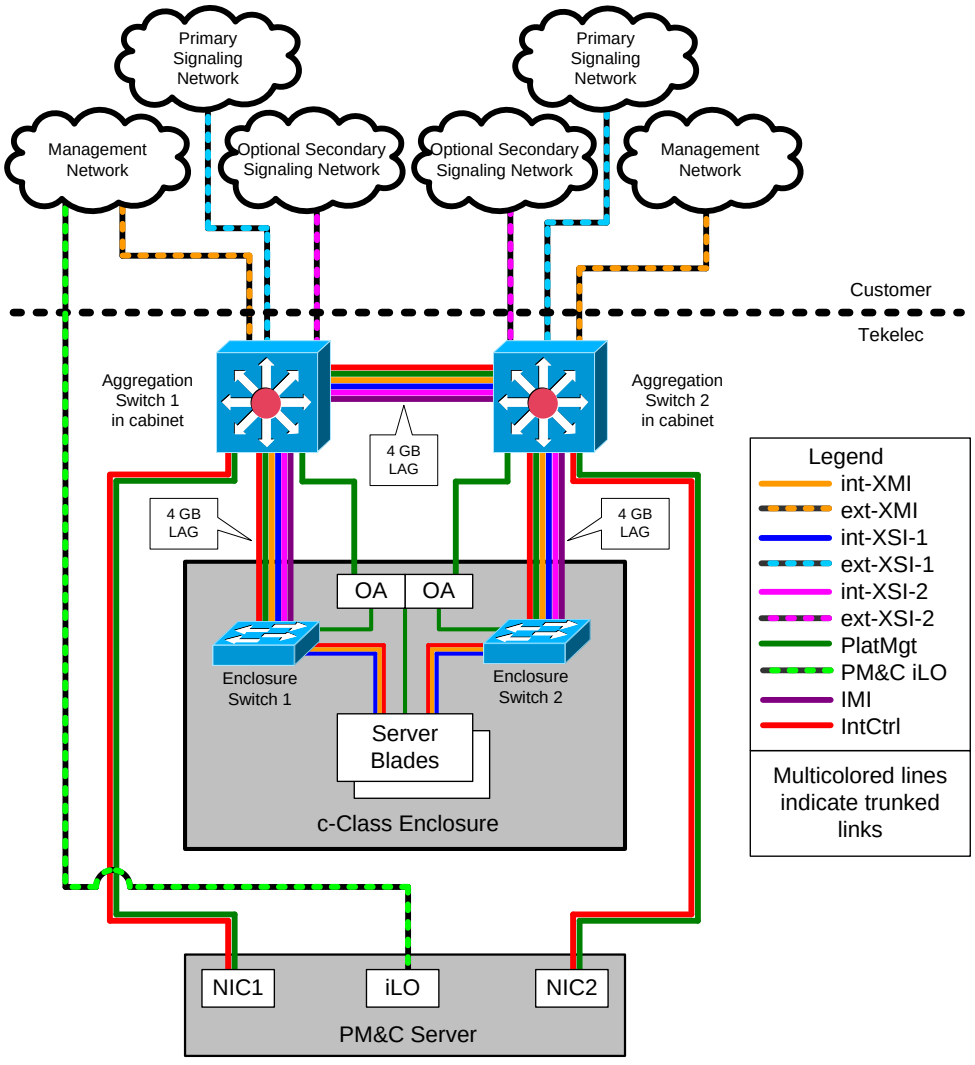
1.3 HIGH LEVEL NETWORKING DESCRIPTION

There are three IP networking options for a C-class system. These are:

- With Cisco 4948 Aggregation (top-of-rack) switch, and Layer 3 uplinks (preferred)
- With Cisco 4948 Aggregation (top-of-rack) switch, and Layer 2 uplinks
- Layer 2 uplinks direct from c-Class Enclosure switches (HP Proliant 6120XG) to customer network, with 10G uplinks.

The decision of what interconnect method will be used is typically made even before the equipment order is placed.

Figure 1: SPR on C-CLASS 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:

- C-CLASS environment setup ready and Network configuration performed on enclosure and aggregation switches. PM&C server application installed.
- 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 OA of the C-CLASS
- 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 an 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 C-CLASS server*

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

Network Name	Identifier	Default VLAN ID	Subnet Size, Mask	Routable	Usage
Control	IntCtrl	1	/24	No	PM&C and server internal control and maintenance
Management	PlatMgt[1]	2	/26	Yes	Management and ILO
OAM/Geo	XMI	3	/27	Yes	External management access and Geo redundancy replication
Internal Messaging	IMI	4	/16	No	Internal Communication Network - Requires 2 static IPs (fixed to 169.254.0.0/16)
Signaling – A	XSI-1	5	/28	Yes	First External Signaling Network
Signaling – B	XSI-2	6	/28	Yes	Second External Signaling Network

Table 3: Network List in C-CLASS server

1.5.2 *XMI configuration*

Table 4: XMI configuration

Description	IP
OAM VLAN ID	XMI_Subnet_ID (default 3)
OAM NETWORK	OAM_NET
OAM Subnet mask	XMI_MASK
OAM Default gateway	XMI_GATEWAY
OAM VIPs for SDM	XMI_SDM_VIP
PROVISIONING VIPs for SDM	PROV_SDM_VIP
OAM Planned IP addresses of SDM servers:	
OAM IP Address for SDM 1	XMI_SDM_1
OAM IP Address for SDM 2	XMI_SDM_2
OAM IP Address for SDM n	XMI_SDM_N
Planned host name of SDM servers:	
Host Name for SDM 1	XMI_SDM_Hostname_1
Host Name for SDM 2	XMI_SDM_Hostname_2
Host Name for SDM n	XMI_SDM_Hostname_N

[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 :

Table 5: XSI-1 configuration

Description	IP
XSI-1 VLAN ID	XSI-1_Subnet_ID (default 5)
XSI-1 NETWORK	XSI-1_NET
XSI-1 Subnet mask	XSI-1_MASK
XSI-1 VIP1	XSI-1_SDM_VIP1
XSI-1 VIP2	XSI-1_SDM_VIP2

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:

Table 6: XSI-2 configuration

Description	IP
XSI-2 VLAN ID	XSI-2_Subnet_ID (default 6)
XSI-2 NETWORK	XSI-2_NET
XSI-2 Subnet mask	XSI-2_MASK
XSI-2 VIP1	XSI-2_SDM_VIP1
XSI-2 VIP2	XSI-2_SDM_VIP2

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:

Table 7: IMI configuration

Description	IP
IMI VLAN ID	IMI _Subnet_ID(default 4)
IMI Subnet mask	255.255.0.0
IMI IP Address for SDM 1	169.254.1.1
IMI IP Address for SDM 2	169.254.1.2
IMI IP Address for SDM n	169.254.1.N

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 (a unique integer in the range 1-16)	SDM_UNIQUE_SLOT_ID

1.6 AUTHENTICATION

1. The usernames and passwords that can login to the ILO in full privilege mode should be known. On an C-CLASS 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 Tekelec TPD installation must be known to the installer.

3. The default password of the “admin” account of the Oracle Tekelec SDM installation must be known to the installer.

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.The TPD and SDM application is performed via PM&C server.

1.8 ACQUIRING FIRMWARE

Procedure Update APPLICATION BLADE FIRMWARE in this document pertains to the upgrading of firmware on SDM blades and hardware devices. The required firmware media and binaries are managed and distributed as part of the HP Solutions Firmware Upgrade Pack 2.2.1, released under Oracle Tekelec Part Number 795-0000-2yy . The current minimum firmware release required for this product is HP Solutions Firmware Upgrade Pack 2.2.1.

The HP Solutions Firmware Upgrade Pack contains multiple BOM items including media and documentation. This document only requires access to the media (CD/DVD or ISOs) as well as the Release Notes document.

The two pieces of required firmware media provided in the HP Solutions Firmware Upgrade Kit 2.2.1 release are:

- HP Smart Update Firmware DVD/ISO - 872-2488-101-2.2.1-10.26.0.iso
- HP Misc Firmware CD/ISO - 872-2161-114-2.2.1_10.27.0.iso

Refer to the Release Notes of the target release of the HP Solutions Firmware Upgrade Pack used to determine specific media part numbers to use and the specific firmware versions provided.

Policy/SDM 9.x Servers and devices that may require firmware updates are:

- HP c7000 Blade System Enclosure Components:
  - Onboard Administrator (Rev 3.50 or greater is REQUIRED to support GEN 8)
  - HP 6120XG Network Switches
  - BL460c Blade Servers
- HP Rack Mount Servers (DL360 / DL380)
- Cisco 4948E-F Rack Mount Network Switch

1.9 C-CLASS CONFIGURATION WITH ADDITIONAL DRIVES

Hardware Configuration		Servers/ site	RAM /server	HD /server (BE)
6352	2 x BL460c (64GB) + 2 x Storage Arrays	2	48GB	2x 600GB in RAID1
6552	2 x BL460c (128GB) + 2 x Storage Arrays	2	64GB	4x (2x 600GB in RAID1)
6654	2 x BL460c (192GB) + 2 x Storage Arrays	2	128GB	4x (2x 600GB in RAID1)
6754	2 x BL460c (64GB)+ 2 x BL460c (256GB)+ 2 x Storage Arrays	4		

Table 8: ***C-CLASS HW configuration types***

2.0 INSTALLATION (AND NETWORKING) IN A C-CLASS ENVIRONMENT

The C-Class environment installation procedures are not within the scope of this doucument.

WI006855 Policy 9.x Sofware Installation Guide covers the procedures to setup the Policy C-Class environment and must be followed from proedure 1 to 15.

2.1 PM&C INSTALLATION

This section provides the procedures to install the PM&C server.

The PM&C server is a rack mount server (DL360/DL380) with an Oracle Tekelec Application that provides tools to manage multiple c-class enclosures and blade software, as well as networking equipment (Aggregation and Enclosure switches) for the c-class environment.

- Procedure 1. Install TVOE 2.0 on Management Server (DL360/DL380)

  PMAC 5.0 is deployed on a Virtual OS (TVOE) environment. The TVOE OS must be installed first, and then the PMAC application iso is installed. PMAC install is not service affecting for the SDM system.

  Note that in SDM Rel 9.x, PMAC is used for Installation activities, growth of new servers and Field repair activities. It is also used for deploying Firmware upgrades.

- Procedure 2. Upgrade DL360/380 Server Firmware

  This procedure upgrade the PM&C DL360 or DL380 server firmware

- Procedure 3. TVOE/Management Server Network Configuration
- Procedure 4. Install PM&C Application

2.2 CONFIGURE AGGREGATION SWITCH

XML configuration files are used as input to the netConfig tool. These must prepared before starting the Installation, as it may take some time to prepare these. See Appendix for instructions on how to prepare these files.

The following procedures use the netConfig tool, with the Xml configuration files, to configure the aggregation switches.

- Procedure 5. Configure PM&C Access to Cisco 4948 Aggregation switch
- Procedure 6. Verify and Update Switch IOS
- Procedure 7. Configure Aggregation Switches with netConfig

2.3 COMPLETE THE PM&C INSTALLATION

- Procedure 8. Configure the PM&C Application

2.4 HP C-7000 ENCLOSURE CONFIGURATION

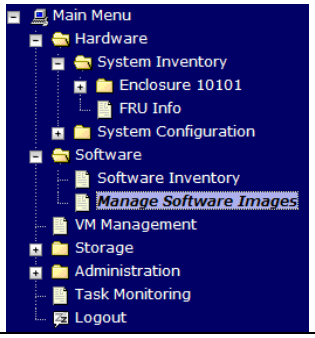
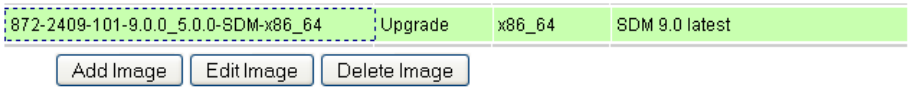
- Procedure 9. Configure OA IP Address (via front panel display)
- Procedure 10. Performing the Initial OA Configuration (OA Configuration Wizard)
- Procedure 11. Adding the Cabinet and Enclosure to PM&C
- Procedure 12. Configuring Enclosure Bay iLO Passwords
- Procedure 13. Configure HP6120XG Enclosure Switches

3.0 LOADING SDM AND TPD SOFTWARE IMAGES ONTO THE PM&C

Procedure 1. Loading Software Images onto the PM&C

S T E P #	This procedure will load the Software Images needed for the SDM/SPR Application onto the PM&C. **Needed material:** - SDM release 9.0 software image 872-2409-101-9.0.0_5.0.0-SDM-x86_64.iso - TPD Image (64 bit) 872-2462-101-7.7.1_1.11.0-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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	Load SPR 9.0 ISO	Insert USB Key containing Software Images into PM&C USB port. Mount the usb to /mnt/upgrade **# mount /dev/sda1 /mnt/upgrade** Verify that there is space in the /var/TKLC/upgrade directory. **# ls /var/TKLC/upgrade** Select Image to transfer: **# ls /mnt/upgrade** Copy a Application Image file to /var/TKLC/upgrade: **# cp /mnt/upgrade/<TPD or Application.iso> /var/TKLC/upgrade** - Alernative: Burn image to DVD, and Insert the Application Image DVD into the removable media drive of the management server. - Alternative: Scp an Application iso file to the management server and place it under **/var/TKLC/upgrade** (if networking is available) # **scp *<ISO_filename>* root@*<pmac_manangement_network_ip>*:/var/TKLC/upgrade**
2. ☐	PM&C GUI: Login	Open web browser and enter: **http://<management_network_ip>** Login as pmacadmin user.

Procedure 1. Loading Software Images onto the PM&C

3. ☐	Navigate to Manage Software Images	Navigate to **Main Menu** -> **Software** -> **Manage Software Images** 
4. ☐	PM&C GUI: Add image	Press **Add Image** button. Use the dropdown to select the image. If the optical media was used in step 1, the device will appear as device://dev/scd0, If the ISO image was copied over in step 1, the device will appear as /var/TKLC/upgrade/872-2409-101-9.0.0_5.0.0-SDM-x86_64.iso  Select the appropriate path and Press **Add New Image** button. You may check the progress using the Task Monitoring link. Observe the green bar indicating success.
5. ☐	Verify Image Loaded	Navigate to **Main Menu** -> **Software** -> **Manage Software Images** Just loaded image will be shown.
6. ☐	Remove image file or Media	Remove the image file from /var/TKLC/upgrade directory. **# ls /var/TKLC/upgrade** **# rm /var/TKLC/upgrade/<image>.iso** **If DVD Media was used, remove this from the drive.**
7. ☐	Add additional images	Repeat above steps to add other images. - Or – **# unmount /mnt/upgrade**

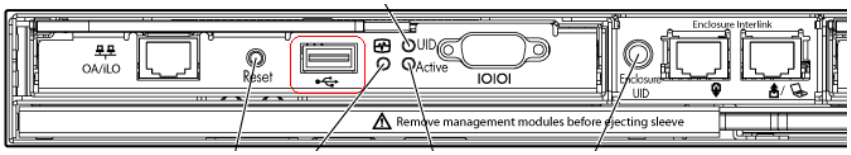
4.0 UPDATE APPLICATION BLADE FIRMWARE

Procedure 2. Update Application Blade Firmware

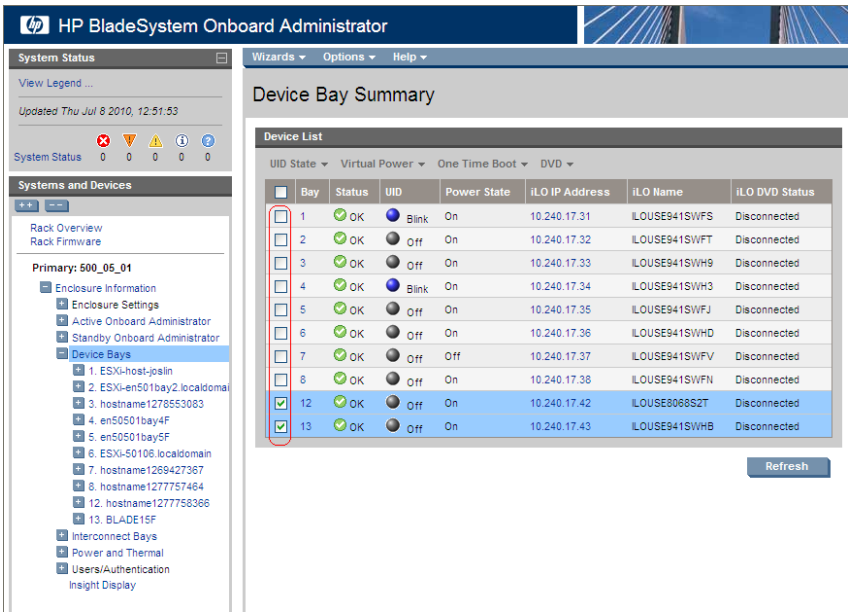
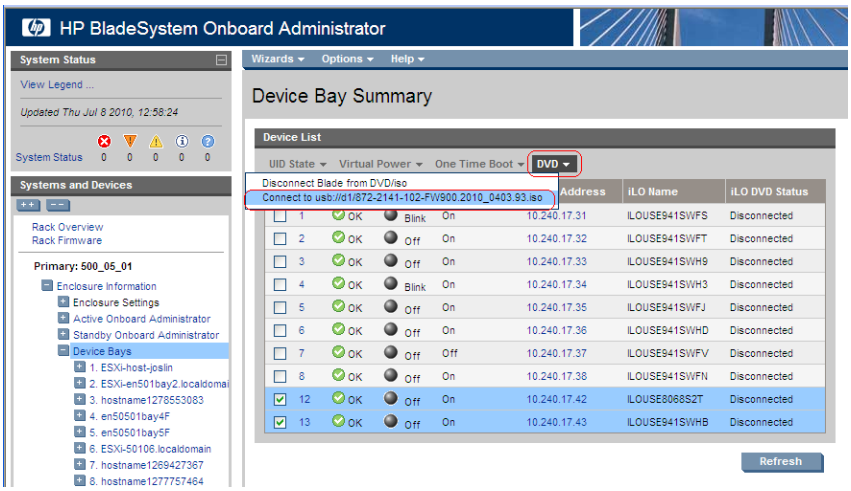
S T E P #		
	This procedure will provide the steps to upgrade the firmware on the SDM Blade servers. The Firmware Update ISO (on a USB key) will be inserted into the Active OA, and then the OA GUI used to apply the update to the blade servers in the Enclosure. At the end of this procedure, some or all the servers in the Enclosure will have the correct Firmware version. NOTE: A Firmware patch (Errata) may also need to be installed on the servers. This can be done after the servers are fully networked (using scp to copy the patch to each server, and execute it). See the HP Solutions Firmware Upgrade Pack Release notes for more information on required Errata. **Prerequisite: *Procedure 13: Configure Enclosure switches*** has been completed. **Needed material:** - HP Smart Update Firmware DVD, **or** ISO file on USB Key - HP Solutions Firmware Upgrade Pack Release Notes **Error! Reference source not found.** 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	Check if Firmware upgrade is needed	Log onto the OA iLO using IE and navigate to **Rack Firmware,** you should be presented with the overview of all components in the enclosure as shown below. Scroll down the view the blades firmware. Check the ROM Version for all the blades in the enclosure. Device Firmware Information If the current verion is at or greater than the minimum supported version, skip this procedure, no upgrade is necessary.
2. ☐	Is ISO available USB?	If you have the HP Smart Update Firmware ISO image on a USB key, then skip to Step 7. Otherwise continue with the next steps to extract the ISO from the DVD.

Bay	Device Model	Firmware Component	Current Version
1	ProLiant BL460c G6	System ROM	I24 05/20/2010
		iLO2	iLO2 2.00 Jun 21 2010
		Power Management Controller	3.4
2	ProLiant BL460c G6	System ROM	I24 05/20/2010
		iLO2	iLO2 2.00 Jun 21 2010
		Power Management Controller	3.4
3	ProLiant BL460c G6	System ROM	I24 05/20/2010
		iLO2	iLO2 2.00 Jun 21 2010
		Power Management Controller	3.4
4	ProLiant BL460c G6	System ROM	I24 05/20/2010
		iLO2	iLO2 2.00 Jun 21 2010
		Power Management Controller	3.4

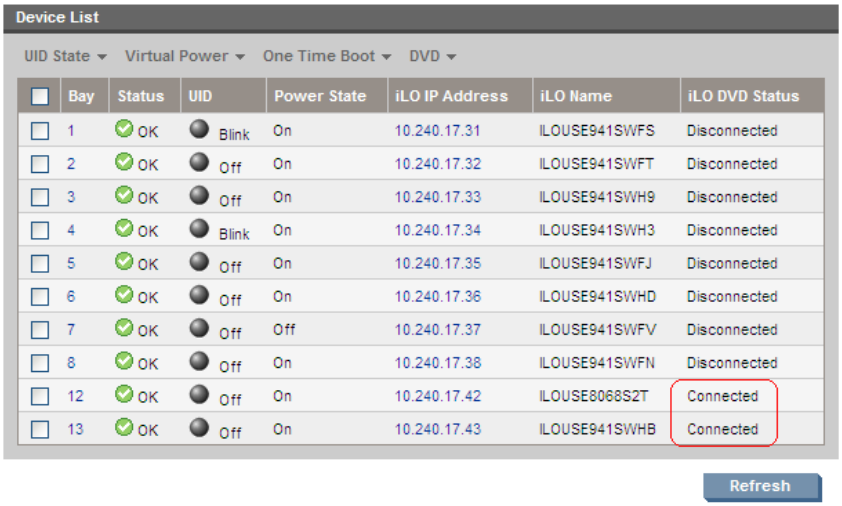
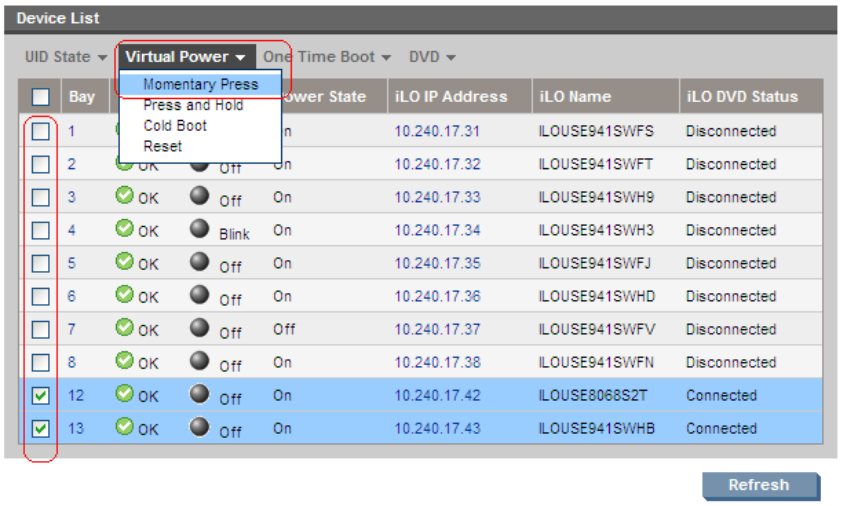
Procedure 2. Update Application Blade Firmware

3. ☐	Import HP Firmware Maintenance CD	Insert the HP Smart Update Firmware DVD into the removable media drive of the management server. Log into the management server shell as the user "root" using ssh. Execute the following command to extract the iso image onto the /var/TKLC/smac/image directory of the PM&C server. (Use the correct iso image part number from HP Solutions Firmware Upgrade Pack Release Notes **Error! Reference source not found.**) # **getCDROM** # **dd if=/dev/scd0 of=/var/TKLC/smac/image/<*image_part_number*>.iso** Verify image extraction completes without error.
4. ☐	Verify extracted image	Verify checksum of the extracted ISO with the value listed in HP Solutions Firmware Upgrade Pack Release Notes **Error! Reference source not found.** # **md5sum /var/TKLC/smac/image/<*image_part_number*>.iso** 422275a25353030fb5338876761ee1ca /var/TKLC/smac/image/872-XXXX-XXX-firmware.iso **Note**: The actual iso image in the output is for illustrative purposes only
5. ☐	Copy HP Firmware Maintenance iso image to laptop	Copy the image from the management server to your laptop using an scp client: /var/TKLC/smac/image/<image_part_number>.iso
6. ☐	Copy ISO to USB Media	Take the ISO you just copied to your laptop and copy it to USB media.
7. ☐	Insert USB Flash Drive	Insert the USB Flash Drive with the *HP Smart Update Firmware* ISO into the USB port of the Active OA Module on Enclosure. (Active OA is indicated by the Active LED) 
8. ☐	Access the Active OA	**Access the Active OA Login Page from an Internet Explorer ® session using the following URL:** **https://<OA_IP>/**
9. ☐	Log in to the Active OALog in as an administrator user.	User Name = <OA_admin_user> Password = <OA_admin_password>

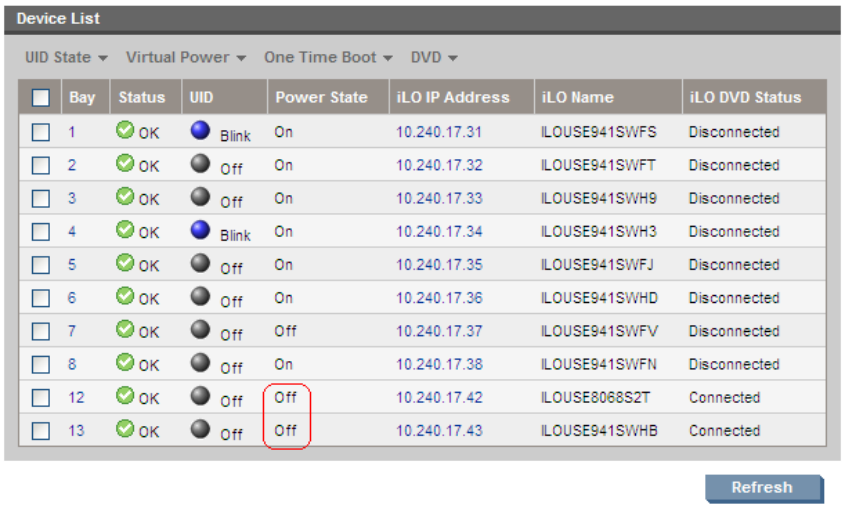
Procedure 2. Update Application Blade Firmware

10. ☐	Access the Device Summary page On the left pane, expand the Device Bays node to display the Device Bay Summary window. Select the individual blades to be upgraded by clicking and enabling the corresponding UID checkbox.	 **Note**: A maximum of 8 blades should be upgraded concurrently at one time. If the c7000 enclosure has more than 8 blades they will need to be upgraded in multiple sessions.
11. ☐	Connect to USB Drive	Once the blades are selected, connect them to the ISO on the USB Drive, by selecting the **Connect to usb…** item from the **DVD** menu. 

Procedure 2. Update Application Blade Firmware

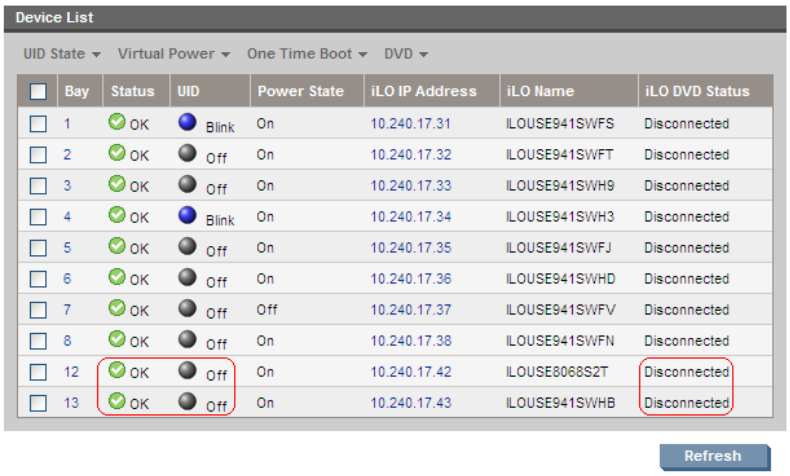
12. ☐	Verify Drive Connection	Once each blade has mounted the ISO media the **Device List** table should indicate an **iLO DVD Status** as *Connected* for each blade that was previously selected.  **Note**: The **Refresh** button may need to be clicked in order to see the current status of all blades.
13. ☐	Power Down Blades	If needed, reselect the UID checkbox for each blade to be upgraded and then select the **Momentary Press** option under the **Virtual Power** menu.  When prompted click the **OK** button to confirm the action.

Procedure 2. Update Application Blade Firmware

14. ☐	Verify Power Down	The power down sequence can take several minutes to complete. When it completes the **Device List** table will indicate the **Power State** of each select blade to be *Off.*  **Note**: The **Refresh** button may need to be clicked in order to see the current status of all blades.
15. ☐	Initiate Firmware Upgrade	To power the blades back on and begin the automated firmware upgrade process, repeat Steps 18 and 19 this time being sure the **Power State** indicates *On* for each selected blade.

Bay	Status	UID	Power State	iLO IP Address	iLO Name	iLO DVD Status
1	OK	Blink	On	10.240.17.31	ILOUSE941SWFS	Disconnected
2	OK	Off	On	10.240.17.32	ILOUSE941SWFT	Disconnected
3	OK	Off	On	10.240.17.33	ILOUSE941SWH9	Disconnected
4	OK	Blink	On	10.240.17.34	ILOUSE941SWH3	Disconnected
5	OK	Off	On	10.240.17.35	ILOUSE941SWFJ	Disconnected
6	OK	Off	On	10.240.17.36	ILOUSE941SWHD	Disconnected
7	OK	Off	Off	10.240.17.37	ILOUSE941SWFV	Disconnected
8	OK	Off	On	10.240.17.38	ILOUSE941SWFN	Disconnected
12	OK	Off	Off	10.240.17.42	ILOUSE8068S2T	Connected
13	OK	Off	Off	10.240.17.43	ILOUSE941SWHB	Connected

Procedure 2. Update Application Blade Firmware

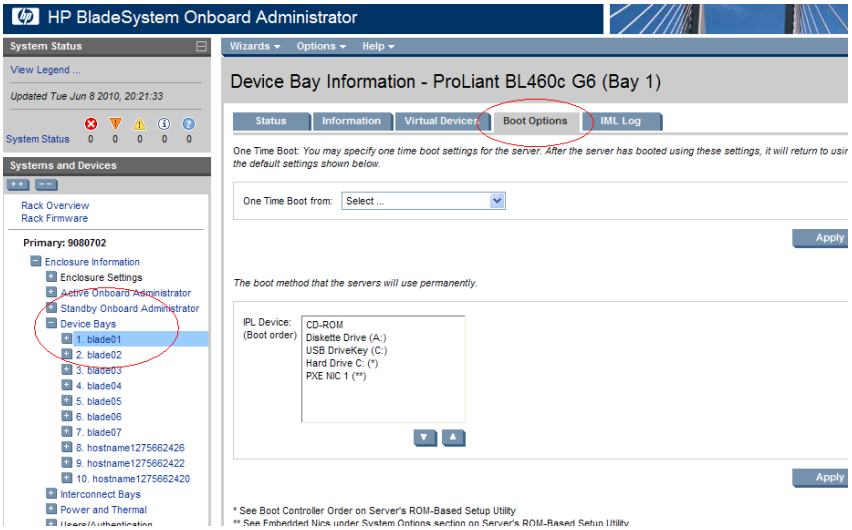
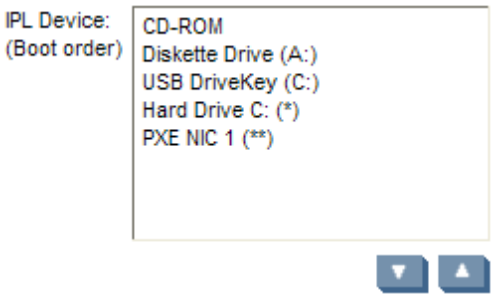
16. ☐	Monitor Firmware Upgrade	From this point on each blade will boot into an automated firmware upgrade process that will last between *20 to 25 minutes*.  Upon a successful firmware upgrade, the **Device List** table will list each blade with a **Status** of *OK*, **UID** of *Off* and the **iLO DVD Status** as *Disconnected.* At this time the blades will automatically be rebooted. If the status does not update to disconnected, you can verify completion by opening an iLo window (via the OA) for each blade and watching the console for indication of firmware upgrade progress and successful completion If necessary, repeat Steps 15 through 21 for the remaining blades in the enclosure to be upgraded. Proceed to the next step.
17. ☐	Remove USB Flash Drive	The USB flash drive may now safely be removed from the Active OA module.
18. ☐	Remove temporary file	After all blade servers have been upgraded, the file copied to laptop in Step 3 may be removed.
19. ☐	Check for Additional Updates	Before proceeding, it is necessary to determine if additional firmware upgrades have been included in the HP Smart Update Firmware DVD/ISO [1] to determine which (if any) HP Errata Firmware Component upgrades must be installed manually
20. ☐	Update Mezzanine Cards Firmware (Optional)	If the blades have mezzanine cards installed, please refer to [1], section 4.10 on how to upgrade the mezzanine cards firmwares.

5.0 ADJUST POWER MANAGEMENT AND INSTALL TPD VIA PM&C

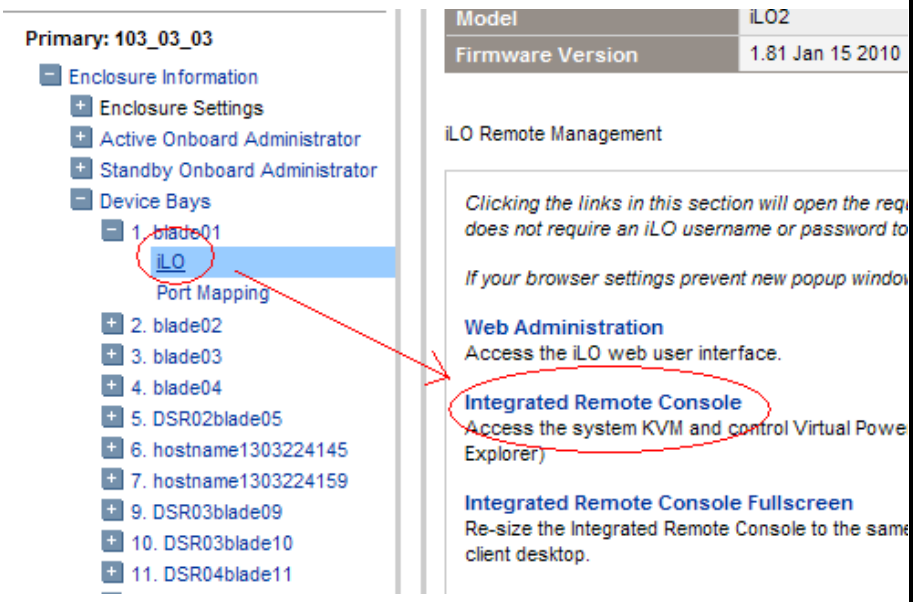
Procedure 3. This procedure install TPD on C-CLASS via PM&C

S T E P #		
	This procedure will install TPD on C-CLASS server and update BIOS settings. **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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	Connect to OA	Open your web browser and navigate to the OA IP address You will see following: Login to HP OA as Administrator. Original password is on paper card attached to each OA.

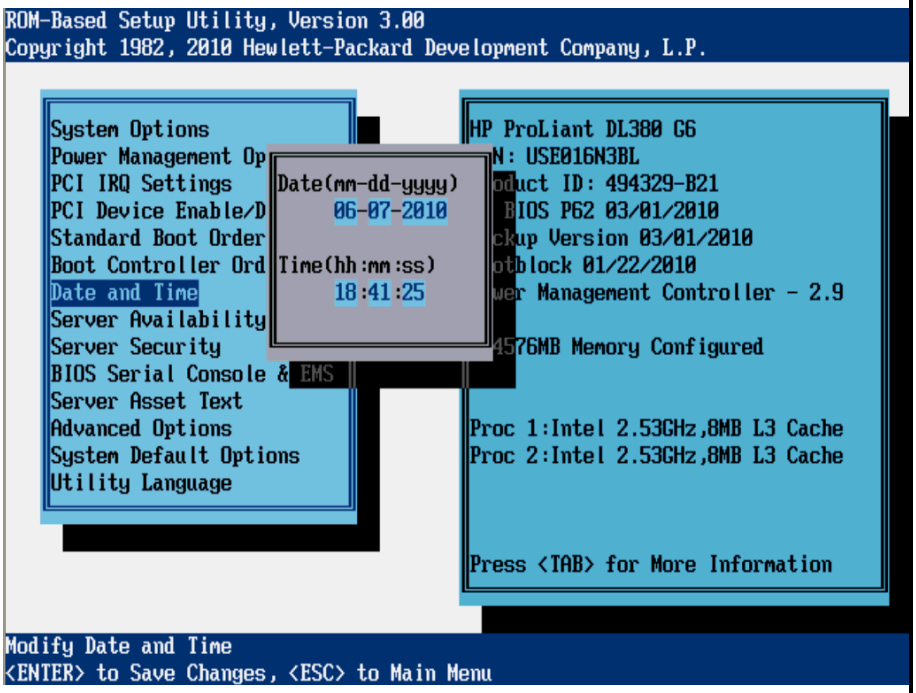
Procedure 3. This procedure install TPD on C-CLASS via PM&C

2. ☐	Navigate to device Bay Settings	Navigate to **Enclosure Information** -> **Device Bays** -> **<Blade 1>** Click on **Boot Options** Tab 
3. ☐	Verify/update Boot device Order	Verify that the Boot order is as follows. If it is not, use the up and down arrows to adjust the order to match the picture below, then click on **Apply** 

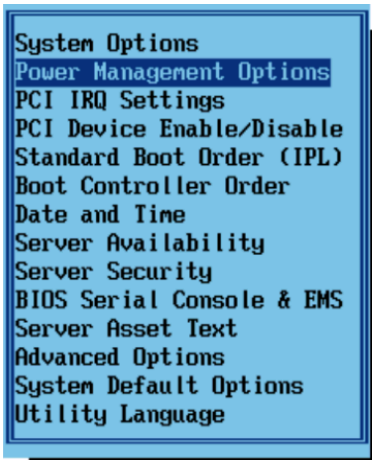
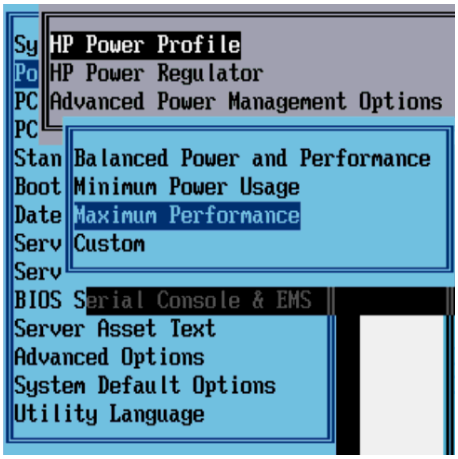
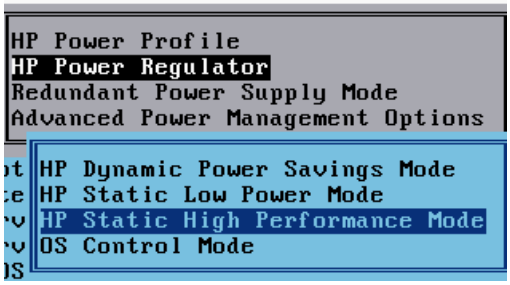
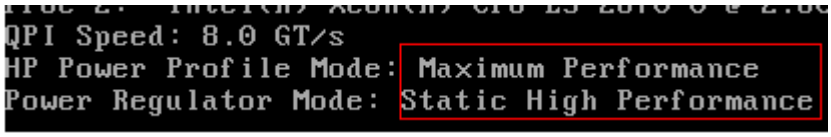
Procedure 3. This procedure install TPD on C-CLASS via PM&C

4. ☐	Access the Blade iLO	Navigate to **Enclosure Information** -> **Device Bays** -> **<Blade 1>** -> **iLO** Click on **Integrated Remote Console**  This will launch the iLO interface for that blade. If this is the first time the iLO is being accessed, you will be prompted to install an addon to your web browser, follow the on screen instructions to do so.
	Restart the blade and access the bios	You might be prompted with a certificate security warning, just press continue. Once a promt is displayed, login onto the blade using the “root” username. Once logged in, Reboot the server (using the “reboot” command) 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.

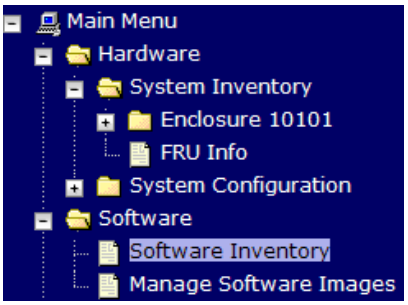
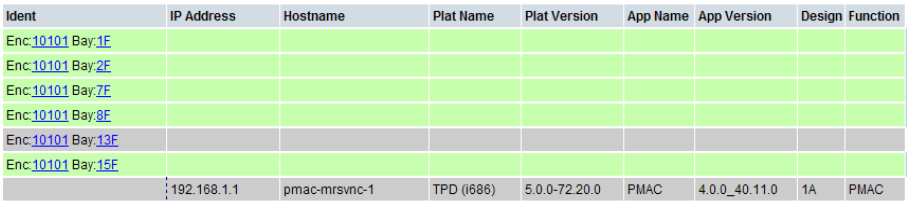
Procedure 3. This procedure install TPD on C-CLASS via PM&C

5. ☐	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. 

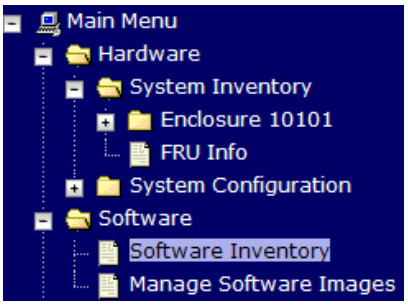
Procedure 3. This procedure install TPD on C-CLASS via PM&C

6. ☐	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 3. This procedure install TPD on C-CLASS via PM&C

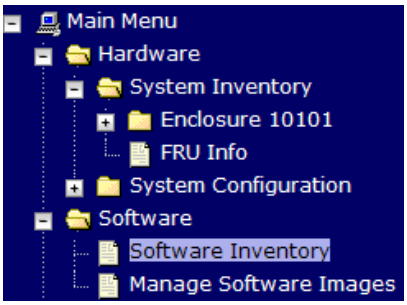
7. ☐	Verify if PM&C Contol Network is established to the blades.	Navigate to **Software** -> **Software Inventory**.   If the PM&C Control network is correctly configured, the PM&C will act as a DHCP server and provide control network addresses in the range of 192.168.1.2 – 255 to the blade servers in the managed cabinets/enclosures. PM&C always takes the address of 192.168.1.1. If the server has requested a IP address from PM&C, the IP address will appear in the “IP Address” column”. TPD will always do this when a server blade is booted, and also periodically after this. If there are no IP Addresses in this view, then either: • PM&C Control Network is not correctly configured (probably a switch config issue) • The Blades do not have a OS installed. If there are IP addresses in this view, then the Contol network is OK. Proceed to next step if there are no IP addresses in the view. Proceed to the next-next step if there are IP addresses in the view.

Procedure 3. This procedure install TPD on C-CLASS via PM&C

8. ☐	Determine if Blades need to be IPM'ed - case: Display is "blank"	Navigate to **Software** -> **Software Inventory**.  If the display is blank, as shown above, then it may be that the blades do not have a OS installed, and it is necessary to IPM the blades. Move to the step (following) to attempt the OS install for one or more blades. NOTE: if the OS Install step fails, then it may be that the Control Network is not correctly established, and trouble shooting will be required.

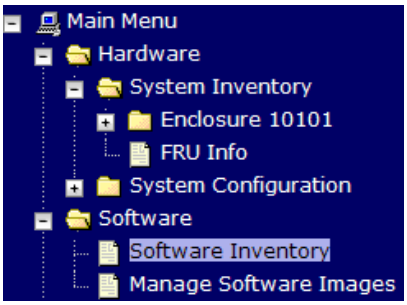
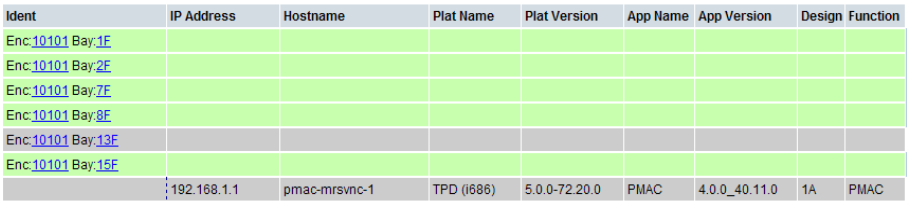
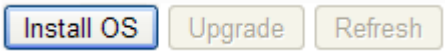
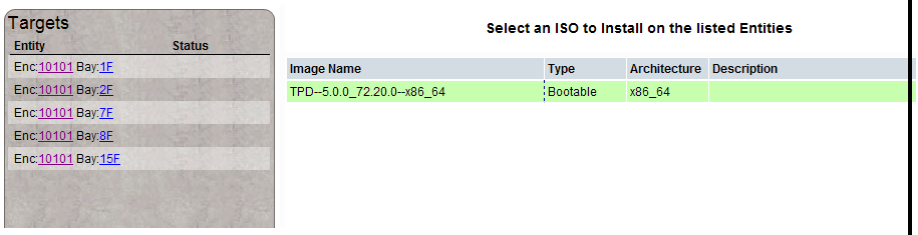
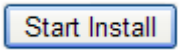
Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version	Design	Function
Enc:10101 Bay:1F								
Enc:10101 Bay:2F								
Enc:10101 Bay:7F								
Enc:10101 Bay:8F								
Enc:10101 Bay:13F								
Enc:10101 Bay:15F								
	192.168.1.1	pmac-mrsvnc-1	TPD (i686)	5.0.0-72.20.0	PMAC	4.0.0_40.11.0	1A	PMAC

Procedure 3. This procedure install TPD on C-CLASS via PM&C

9. ☐	Determine if Blades must be IPM'ed - case: IP Addresses and other information is shown.	Navigate to **Software** -> **Software Inventory**.  If the Control network is established, and the blades have a OS installed (TPD), then PM&C gathers the current software information from the blades, and displays it in this list. • If the display shows an IP address (192.168.1.x), and PlatName = TPD, and Plat Version= xxxxx, then the blade is already installed with a version of the TPD OS. The version of TPD installed on the blades is usually not so important, as long as it is a 64 bit version and not newer than the required version for the Application.. The SDM Application Install (Upgrade action on the PM&C GUI), to be performed in the next procedures, will automatically upgrade the TPD version on the blade to the correct version for the Application. i.e. the 872-2409-101-9.0.0_5.0.0-SDM-x86_64.iso iso includes the TPD version that the Application needs, and the Application install will automatically upgrade the blade TPD (if needed) before it installed the Application. If the version of OS installed on the blade is the same as what is required by the application, then the install will proceed more quickly because it does not need to upgrade TPD. If the Inventory form does not not show a OK version of the TPD on the server, then the OS Install action is needed to install a appropriate version of TPD.

Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version	Design	Function
Enc:10101 Bay:1F								
Enc:10101 Bay:2F								
Enc:10101 Bay:7F								
Enc:10101 Bay:8F								
Enc:10101 Bay:13F								
Enc:10101 Bay:15F								
	192.168.1.1	pmac-mrsvnc-1	TPD (i686)	5.0.0-72.20.0	PMAC	4.0.0_40.11.0	1A	PMAC

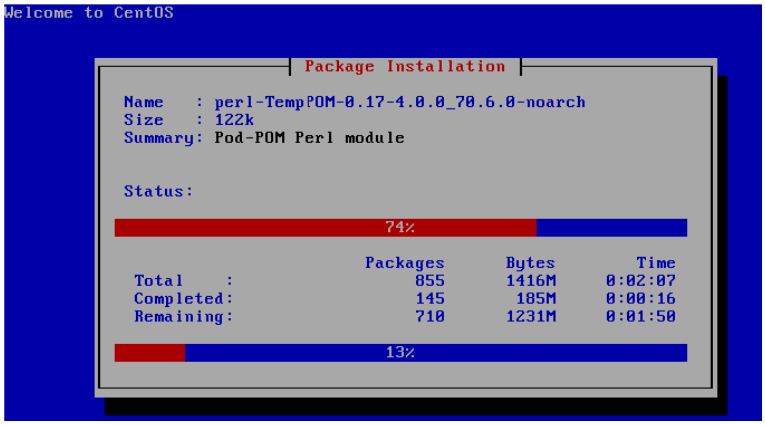
Procedure 3. This procedure install TPD on C-CLASS via PM&C

10. ☐	Select Servers for OS install	Navigate to **Software** -> **Software Inventory**.  Select the SDM blades to IPM (Back-end and Front-end blades if any). Selected rows will be highlighted in green. Note: IPM is also a useful recovery procedure if a server is in a bad or unknown condition, or was configured with a different application, since the IPM will clean all the existing software and disk configurations off of the server, and bring the server to a clean state.  Click on **Install OS** 
11. ☐	Initiate OS Install	The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.  Click on **Start Install**, a confirmation window will pop up, click on **Ok** to proceed with the install. 

Procedure 3. This procedure install TPD on C-CLASS via PM&C

<table>
<tr>
<td>12. ☐</td>
<td>Monitor OS Install</td>
<td>Navigate to Main Menu > Task Monitoring to monitor the progress of the OS Installation background
task. A separate task will appear for each blade affected.
<table>
<tr><th></th><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr>
<tr><td></td><td>14</td><td>Install OS</td><td>Enc:10101 Bay:15F</td><td>Boot install image</td><td>0:00:01</td><td>2011-09-20 11:12:02</td><td>50%</td></tr>
<tr><td></td><td>13</td><td>Install OS</td><td>Enc:10101 Bay:8F</td><td>Boot install image</td><td>0:00:01</td><td>2011-09-20 11:12:02</td><td>50%</td></tr>
<tr><td></td><td>12</td><td>Install OS</td><td>Enc:10101 Bay:7F</td><td>Boot install image</td><td>0:00:01</td><td>2011-09-20 11:12:02</td><td>50%</td></tr>
<tr><td></td><td>11</td><td>Install OS</td><td>Enc:10101 Bay:2F</td><td>Boot install image</td><td>0:00:01</td><td>2011-09-20 11:12:02</td><td>50%</td></tr>
<tr><td></td><td>10</td><td>Install OS</td><td>Enc:10101 Bay:1F</td><td>Boot install image</td><td>0:00:02</td><td>2011-09-20 11:12:01</td><td>50%</td></tr>
<tr><td></td><td>9</td><td>Add Image</td><td></td><td>Done: TPD.install-5.0.0_72.20.0-CentOS5.6-x86_64</td><td>0:00:09</td><td>2011-09-20 11:01:50</td><td>100%</td></tr>
</table>

You can also monitor the install from the blade iLo :



When the installation is complete, the task will change to green and the Progress bar will indicate "100%".</td>
</tr>
<tr>
<td></td>
<td>IF OS Install fails</td>
<td>If the OS Install Fails, the Task status will show failed.

Note the step where the Installed failed.

It is also useful to login the server console (either via the iLo port, or using a local Key Board and Monitor), and try the OS Install again. Note where the console is reporting a boot problem.

If the boot hangs when trying to get a DHCP address, and execute PXE boot, then the Control Network is a problem.

Trouble shoot the IP networking before proceeding.</td>
</tr>
</table>

6.0 BASIC POST INSTALL CONFIGURATION OF TPD ON EACH C-CLASS SERVER

Procedure 4. SDM pre-installation specific steps.

S T E P #	Steps to be completed.	This installation must be repeated for each C-CLASS blade planned to be part of the SDM/TPD configuration.It describes how to configure the network interfaces,NTP,RAID1 used by SDM SPR system.The disk configuration has to be performed only on Back-End blades. **Needed material:** - 2 D2200sb storage blades with 12 Additional 600GB Physical Drives for C-CLASS configurations with Storage arrays. 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.
1 ☐	Edit network file on SDM On all blades	Using SSH or the Console of each C-CLASS 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 C-CLASS server hostname on On all SDM blades	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**

<table>
<tr><td></td><td></td><td>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</td></tr>
<tr><td>3 ☐</td><td>Change server Time Zone on all SDM blades.</td><td>Use the TPD menu front-end to set the server's Time Zone:

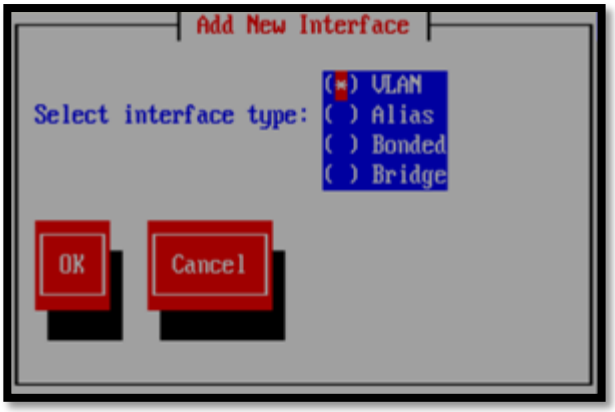
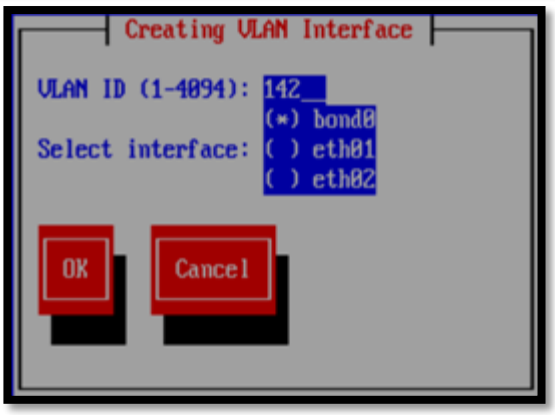
su - platcfg

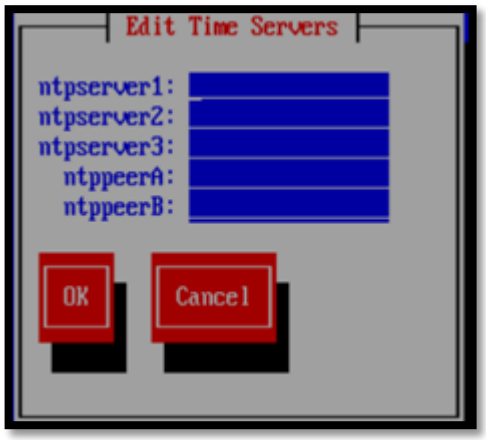
navigate through Main Menu -> Server Configuration -> Time Zone use the "Edit" button to change the Time Zone

navigate the menus back to the main menu and Exit

The System Clock uses UTC, MUST BE SELECTED

• Verify the date :
date</td></tr>
<tr><td>4</td><td>Create the vlan interfaces from platcfg menu on all SDM blades.</td><td>Navigate through the main menu and create the folowing vlan interfaces.
<table><tr><th>Network Name</th><th>Identifier</th><th>VLAN ID</th></tr><tr><td>Management</td><td>PlatMgt</td><td>bond0.2</td></tr><tr><td>OAM/Geo</td><td>XMI</td><td>bond0.3</td></tr><tr><td>Internal Messaging</td><td>IMI</td><td>bond0.4</td></tr><tr><td>Signaling – A</td><td>XSI-1</td><td>bond0.5</td></tr><tr><td>Signaling – B</td><td>XSI-2</td><td>bond0.6</td></tr></table></td></tr>
</table>

		Main Menu -> Network Configuration -> Network Interfaces -> IPv4 -> Add an Interface -> VLAN VLAN ID: **XMI_Subnet_ID** Select Interface Type: **VLAN** Select interface: **bond0**   • Navigate the menus back to the main menu and Exit • Set in Bond0 MII Monitor Interval to 30 **# netAdm set --device=bond0 --miimon=30** Interface bond0 was updated Interface bond0 updated • Verify **# more /proc/net/bonding/bond0**
5 ☐	Configure IMI interface on each SDM blade.	**Assign an IP address to bond0.4 interface.** **# netAdm set --device=bond0.4 --address= IMI_SDM_TPD_IP_X --netmask= IMI_MASK --onboot=yes**

		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)
6	Configure XMI interface on each SDM blade.	**Assign an IP address to bond0.3 interface.** **# netAdm set --device=bond0.3 --address= XMI_SDM_TPD_IP_X --netmask= XMI_MASK --onboot=yes**
7	Configure XMI gateway as the default route on each SDM blade.	Configure the default route to gateway **XMI_GATEWAY**: **#netAdm add --route=default --device=bond0.3** **--gateway=XMI_GATEWAY** 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*
8 ☐	Configure NTP server address on SDM On all back-end blades	• 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** 

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

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:

<pre>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</pre>

The offset with the reference clock shoul be close to 0.000.

</td>
</tr>
<tr>
<td>9 ☐</td>
<td>Create the required SDM RAID1+0 setup on SDM on all back-end blades</td>
<td>
Create the RAID configuration from Raid controller menu (only for configuration with additional hard drives/storage blades).

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 3 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:

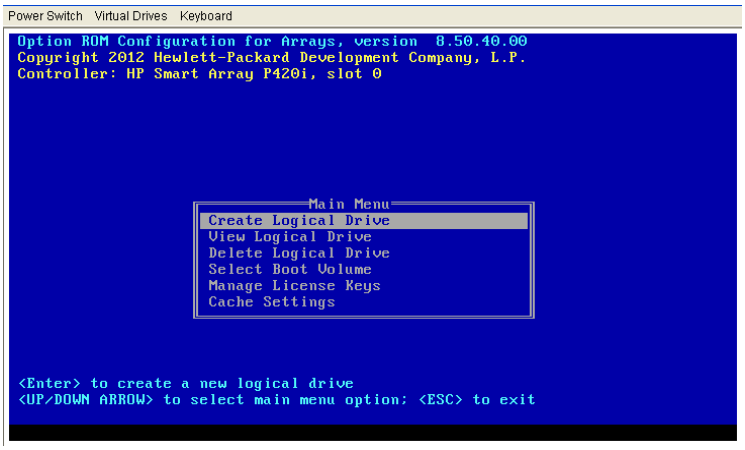
Disk Bay 1&2&3&4 : RAID1+0
Disk Bay 5&6&7&8 : RAID1+0

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

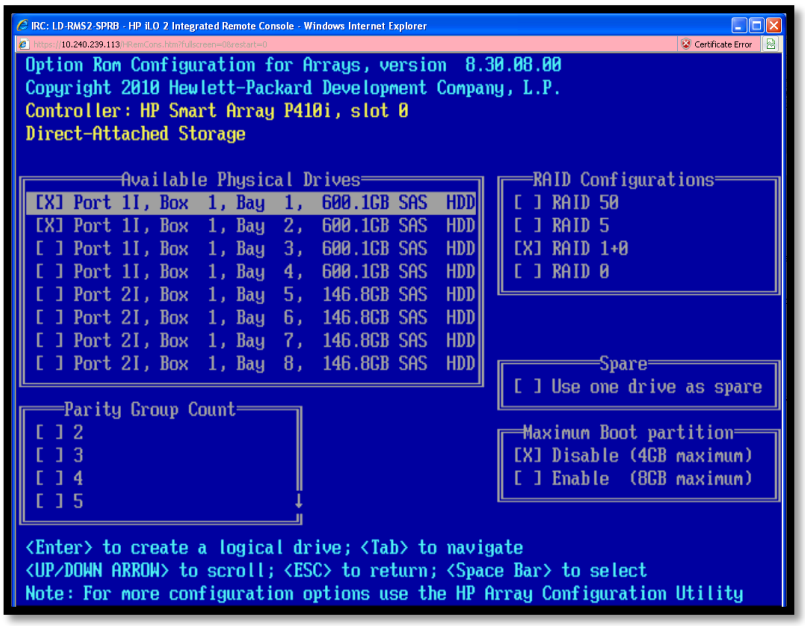
<table>
<tr>
<td></td>
<td></td>
<td>

- **Disk Bay 9&10&11&12 : RAID1+0**

- 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 :

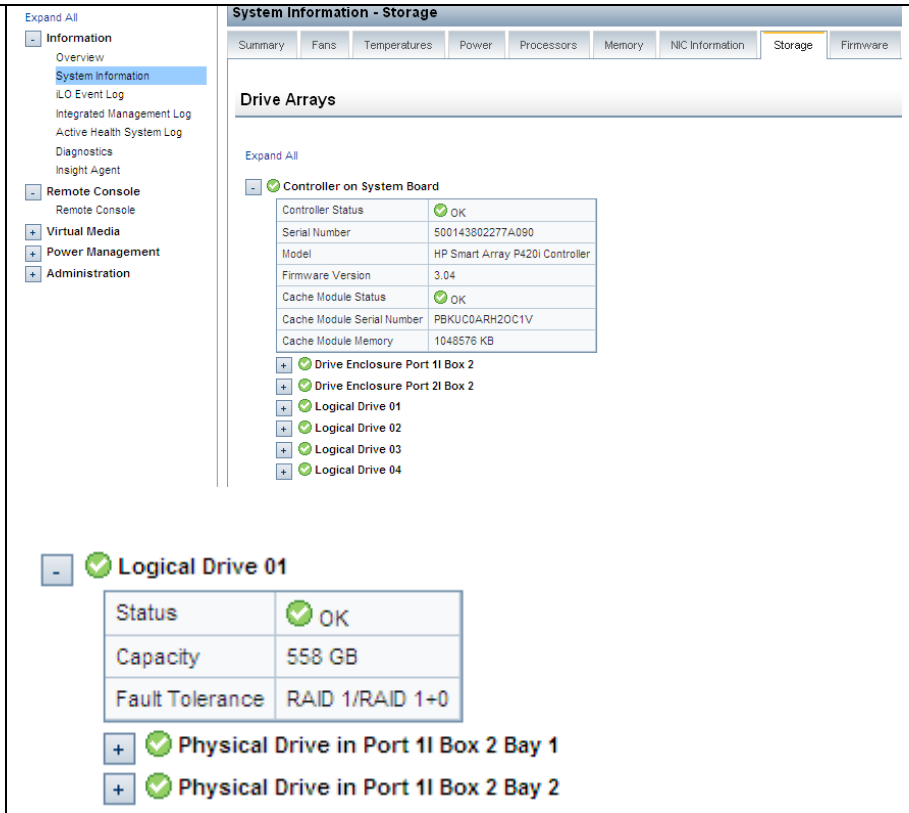


Press F8 to save the configuration:

- Repeat the process for the other 8 drives:

- Once the RAID1+0 configuration is completed, press <ESC> to exit and let the blade boot normally..

</td>
</tr>
<tr>
<td>10 ☐</td>
<td>Verify the Drive Array configuration from the iLO4.</td>
<td>Check the 4 logical drives From the iLO4 menu Information => System Information under storage :</td>
</tr>
</table>


Expand All
Information
Overview
System Information
iLO Event Log
Integrated Management Log
Active Health System Log
Diagnostics
Insight Agent
Remote Console
Remote Console
Virtual Media
Power Management
Administration
System Information - Storage
Summary
Fans
Temperatures
Power
Processors
Memory
NIC Information
Storage
Firmware
Drive Arrays
Expand All
Controller on System Board
Controller Status
OK
Serial Number
500143802277A090
Model
HP Smart Array P420i Controller
Firmware Version
3.04
Cache Module Status
OK
Cache Module Serial Number
PBKUC0ARH2OC1V
Cache Module Memory
1048576 KB
Drive Enclosure Port 1I Box 2
Drive Enclosure Port 2I Box 2
Logical Drive 01
Logical Drive 02
Logical Drive 03
Logical Drive 04

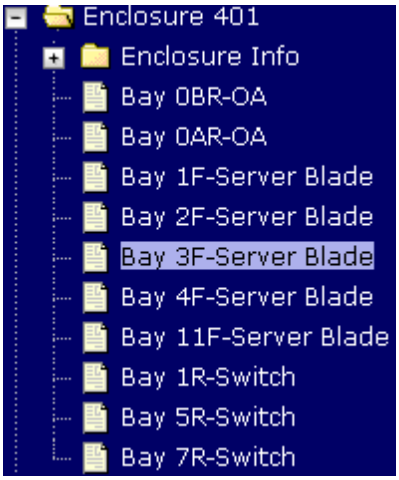
Logical Drive 01
Status
OK
Capacity
558 GB
Fault Tolerance
RAID 1/RAID 1+0
Physical Drive in Port 1I Box 2 Bay 1
Physical Drive in Port 1I Box 2 Bay 2

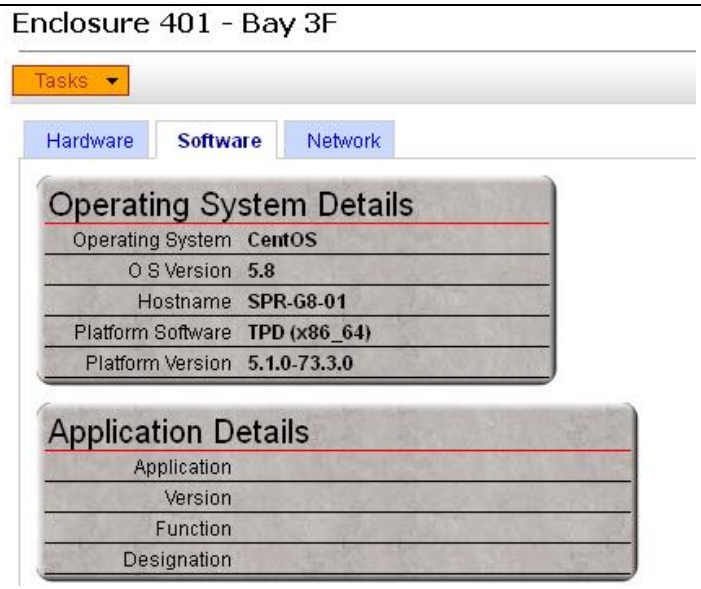
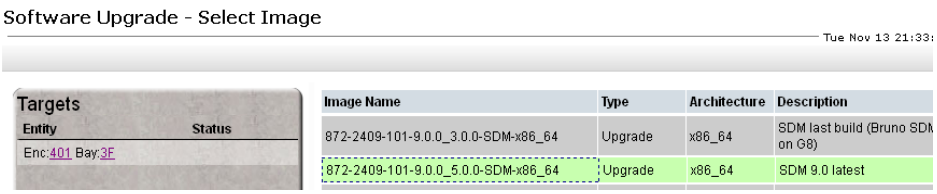
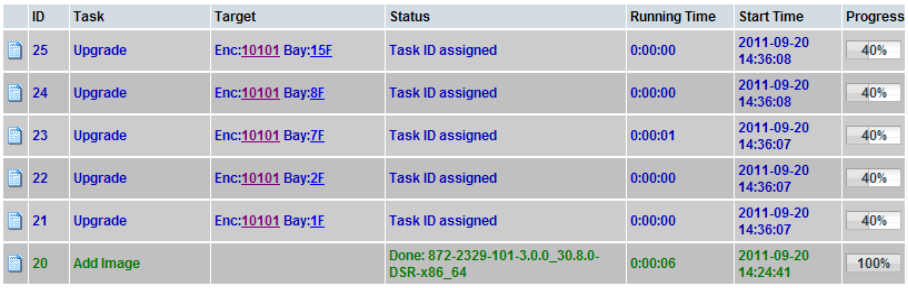
7.0 BASIC INSTALLATION AND CONFIGURATION OF SDM SOFTWARE

Procedure 5. SDM Installation

S T E P #	Steps to be completed.	This installation must be repeated for each C-CLASS 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.
1 ☐	Edit blue file on all SDM blades.	Using SSH or the virtual console of each C-CLASS 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_CC1 SHELFID=1 **SLOTID=1** PRIVATEINTERFACE=bond0 PUBLICINTERFACE=bond2 SINGLEFRAGMENTDB=1 INNODBBUFFERPOOL=**0.7** Example of Blue File in SDM Server B SYSTEMTYPE=RACKMOUNT SITENAME=CSLAB_CC1 SHELFID=1 **SLOTID=2** PRIVATEINTERFACE=bond0 PUBLICINTERFACE=bond2 SINGLEFRAGMENTDB=1 INNODBBUFFERPOOL=**0.7** For Geo-Redundancy Only Note: If geo-redundancy is used, file /etc/sysconfig/blue must contain two extra lines: For C-CLASS servers in **SDM1 (site 1)**, the two extra lines in file /etc/sysconfig/blue should be: SITESUFFIX=_1 SITESUFFIXREMOTE=_2 For C-CLASS 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 active system controller.	• Prepare a sdm-vlans.conf file for the SDM installation. • Using SSH or the virtual console of each C-CLASS 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** 10.223.65.128 27 255.255.255.224 10.223.65.129 bond0 5 **xsi1** # XSI network for Benfica 10.223.65.128 27 255.255.255.224 10.223.65.129 bond0 5 **main** 10.223.64.128/27 # XSI network for San Andre 10.223.65.128 27 255.255.255.224 10.223.65.129 bond0 5 **main** 10.192.211.128/27 10.223.65.64 26 255.255.255.192 10.223.65.65 bond0 3 **xmi** 10.223.65.64 26 255.255.255.192 10.223.65.65 bond0 3 **xmi** 10.192.212.38/32 PREFSRC 10.223.65.102 10.223.65.64 26 255.255.255.192 10.223.65.65 bond0 3 **main** 10.192.212.38/32 PREFSRC 10.223.65.102 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 [TK5] 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 On all back-end blades	• 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 ☐	Select Blade for SDM Application install	Navigate to **Cabinet**->**Enclosure** -> **Bay xx – Server Blade**  Select **Software** Tab

		 Click **Upgrade** Select the SDM iso 872-2409-101-9.0.0_5.0.0-SDM-x86_64.iso :  Click **Start Upgrade**
5 ☐	Monitor the SDM installation status	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the SDM/SPR Installation.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%".

ID	Task	Target	Status	Running Time	Start Time	Progress
25	Upgrade	Enc:10101 Bay:15F	Task ID assigned	0:00:00	2011-09-20 14:36:08	40%
24	Upgrade	Enc:10101 Bay:8F	Task ID assigned	0:00:00	2011-09-20 14:36:08	40%
23	Upgrade	Enc:10101 Bay:7F	Task ID assigned	0:00:01	2011-09-20 14:36:07	40%
22	Upgrade	Enc:10101 Bay:2F	Task ID assigned	0:00:00	2011-09-20 14:36:07	40%
21	Upgrade	Enc:10101 Bay:1F	Task ID assigned	0:00:00	2011-09-20 14:36:07	40%
20	Add Image		Done: 872-2329-101-3.0.0_30.8.0-DSR-x86_64	0:00:06	2011-09-20 14:24:41	100%

6 ☐	Verify the Software version and the platform version	Once the reboot and installation are completed,run the following command on the SDM blade. 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 active system controller blade)	**Only do the steps if this C-CLASS 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 C-CLASS 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.

8.0 PERFORM SSH KEYS EXCHANGE

Procedure 6. SDM ssh configuration

STEP #	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 TEKELEC 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**

9.0 CONFIGURE SPR APPLICATION

Procedure 7. SDM disks configuration and SPR application installation

S T E P #	Steps to be completed.	This proceduremust be repeated for each C-CLASS blade 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.**
1 ☐	Create SDM Partitions *(only if additional disks are used)*	If the C-CLASS 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** Succesfull 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/c1d0p2 LV Name /dev/vgroot/plat_tmp Physical volume /dev/cciss/c1d0p2 LV Name /dev/vgroot/plat_var Physical volume /dev/cciss/c1d0p2 LV Name /dev/vgroot/plat_var_tklc Physical volume /dev/cciss/c1d0p2 LV Name /dev/vgroot/plat_usr Physical volume /dev/cciss/c1d0p2 LV Name **/dev/vgroot/SDM** Physical volume **/dev/cciss/c1d0p2** LV Name **/dev/vgroot/SDMBin** Physical volume **/dev/cciss/c0d0p1** LV Name **/dev/vgroot/SDMDb** Physical volume **/dev/cciss/c0d1p1** LV Name **/dev/vgroot/SDMLog**

Physical volume **/dev/cciss/c0d2p1**

- Check that the SDM partitions have been created

```
Filesystem            Size  Used Avail Use% Mounted on
dev/mapper/vgroot-plat_root 992M  293M  649M  32%  /
/dev/mapper/vgroot-plat_tmp 992M   34M  908M   4% /tmp
 /tmp/dev/mapper/vgroot-plat_var 992M  101M  841M  11% /var
 /var /dev/mapper/vgroot-plat_var_tklc 3.9G  1.1G  2.7G  29%  /var/TKLC
/var/TKLC /dev/mapper/vgroot-plat_usr 3.9G  1.7G  2.1G  44%  /usr
/usr /dev/cciss/c1d0p1     251M   22M  217M   9%  /boot
tmpfs                 48G     0   48G   0% /dev/shm
/dev/mapper/vgroot-SDM                540G   40G  472G   8% /var/TKLC/SDM
/dev/mapper/vgroot-SDMBin             270G  188M  256G   1% /var/TKLC/SDMBin
/dev/mapper/vgroot-SDMDb              270G  260M  256G   1% /var/TKLC/SDMDb
/dev/mapper/vgroot-SDMLog             270G  2.2G  254G   1% /var/TKLC/SDMLog
```

Filesystem	Size	Physical volume	LV name	partition		So
/dev/mapper/vgroot-SDM	540GB	c1d0p2	/dev/vgroot/SDM	/var/TKLC/SDM		
/dev/mapper/vgroot-SDMBin	270GB	c0d0p1	/dev/vgroot/SDMBin	/ var/TKLC/SDMBin		/bl
/dev/mapper/vgroot-SDMDb	270GB	c0d1p1	/dev/vgroot/SDMDb	/ var/TKLC/SDMDb		/b
/dev/mapper/vgroot-SDMLog	270GB	c0d2p1	/dev/vgroot/SDMBinLog	/var/TKLC/SDMBinLog		/bl

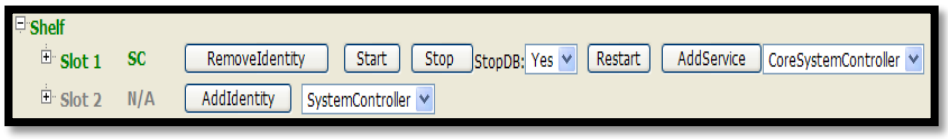
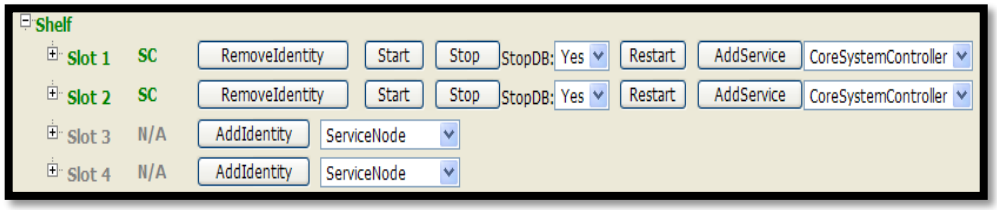
2 ☐ Start the blue Services on SDM server A on SDM1 site

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

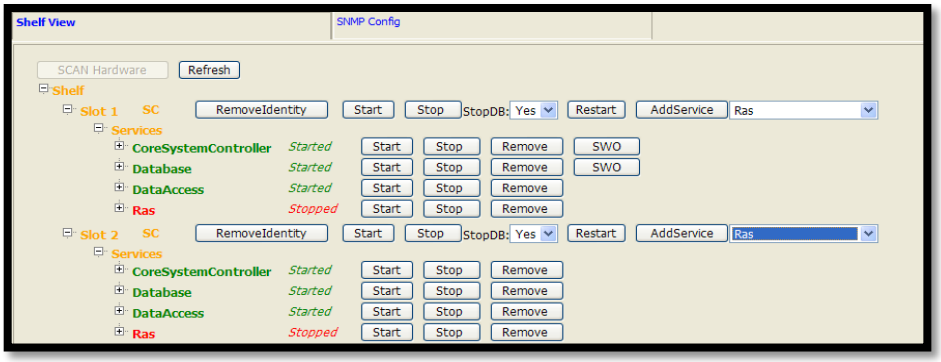
		http://XMI_SDM_VIP_IP:8080 using the IP address of the 1st C-CLASS server on which SDM is installed. • Verify the value of SDM_TPD_UNIQUE_SLOT_ID_X that is configured in file /etc/sysconfig/blue on that system. • In the **WebCI interface**, define the Slot ID of that system as a System Controller **Oracle Tekelec 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	For all subsequent blade servers manually do the first start of the SDM services:

	Standby SDM Blade Server	**# 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 Tekelec SDM™ → System - ID:→ Shelf View**

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

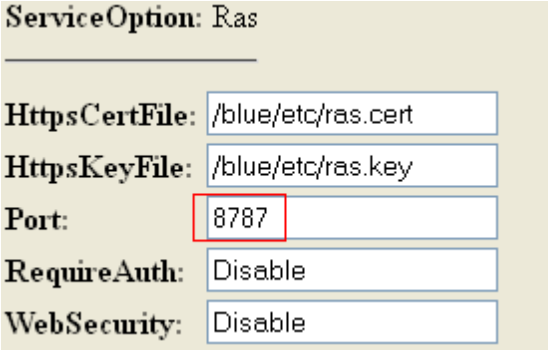
Got to the far right pull down and select the Ras service
Select Add Service on Slot 1 and Slot 2



</td></tr>
<tr><td>9</td><td>Configure the Ras options</td><td>
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 the Oracle Tekelec SDM™ → Service Management:→ Option



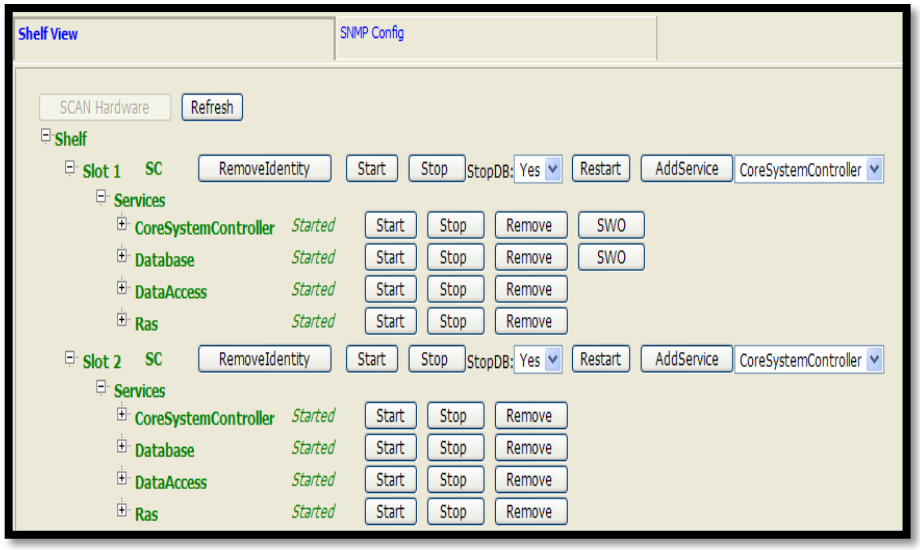
Specify the certificates and key files for HTTPS (HttpsCertFile, HttpsKeyFile)
Enable HTTPS if required ; WebSecurity: Enable
Enable HTTP Authentication if required
Change the Ras port if reauired (default 8787)

<u>Update the changes :</u>

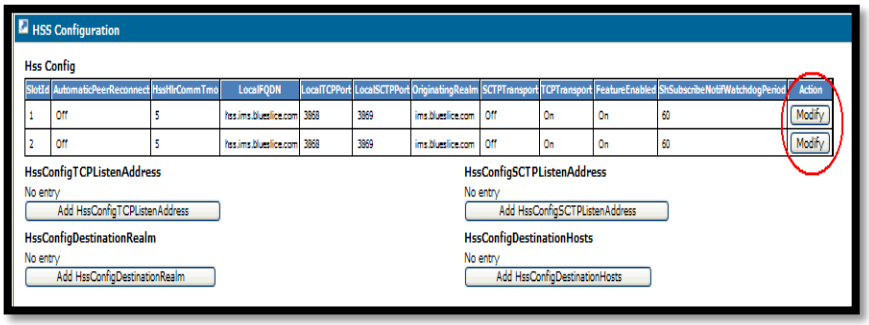
<u>Start Ras services :</u>

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

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

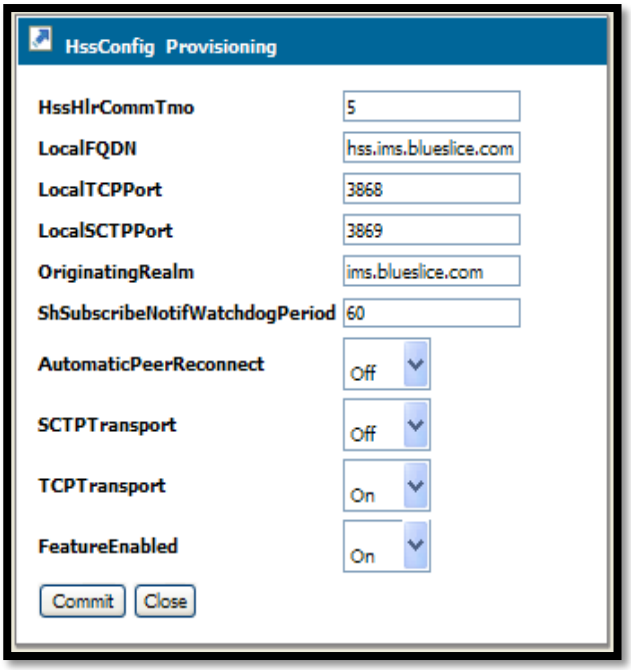
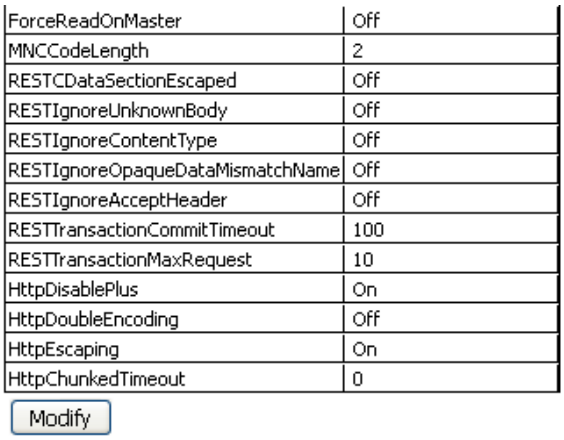
<table>
<tr>
<td></td>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>10 ☐</td>
<td>Add HSS services manually</td>
<td>

Add the HSS service using the same proccess as the Ras

- Configure the Hss Config parameters such as LocalFQDN,localTCPPort,OriginatingRealm, etc
Oracle Tekelec SDM™ → HSS→ HSS Configuration


Modify

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

<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
 
</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:

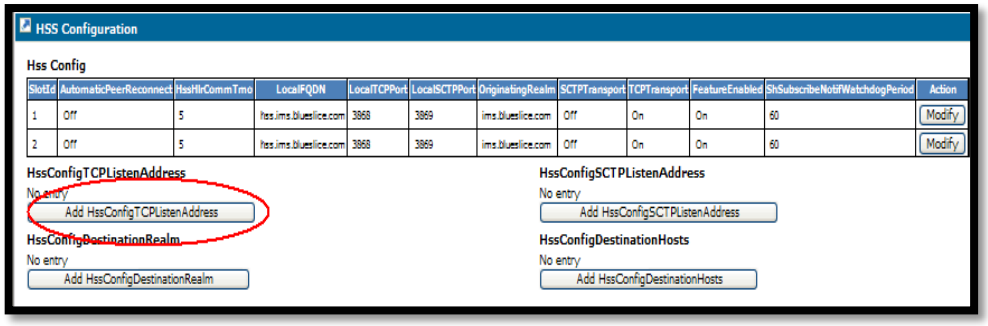
bash /export/Add_codewords.sh

*** 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 on all back-end blades
/opt/OC/bin//oclicoam show max all

Expected output :

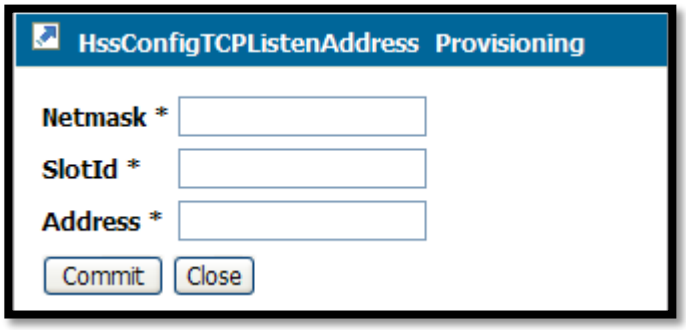
Feature Amount Version ExpiryD
ate
------- ------- ---------- ----------
OcDiamAuth 1 1.3 Unlimited
OcDiamTps 800 1.3 Un
limited
</td>
</tr>
<tr>
<td>13</td>
<td>Configure Sh interface</td>
<td>Configure the Sh Signaling IPs on 1st and 2nd SDM Blade Server (XSI-1 IP adresses and eventually XSI-2)
Oracle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

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


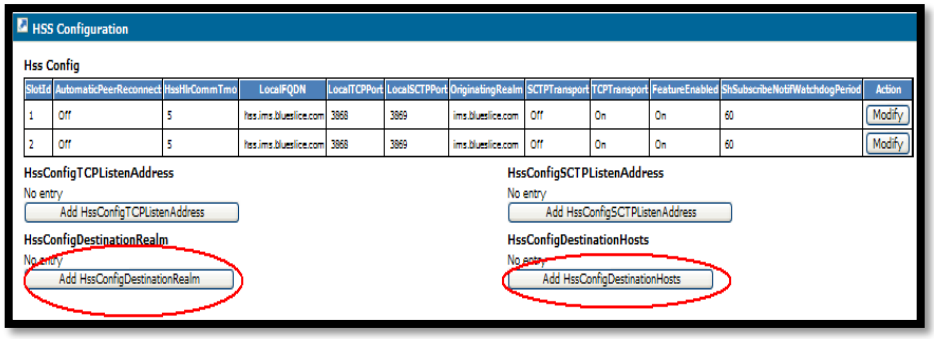
Netmask: XSI-1_MASK

SlotId: SDM_UNIQUE_SLOT_ID

Address: XSI-1_SDM_VIP



Configure the Destination diameter peer parameters (realm,hosts)

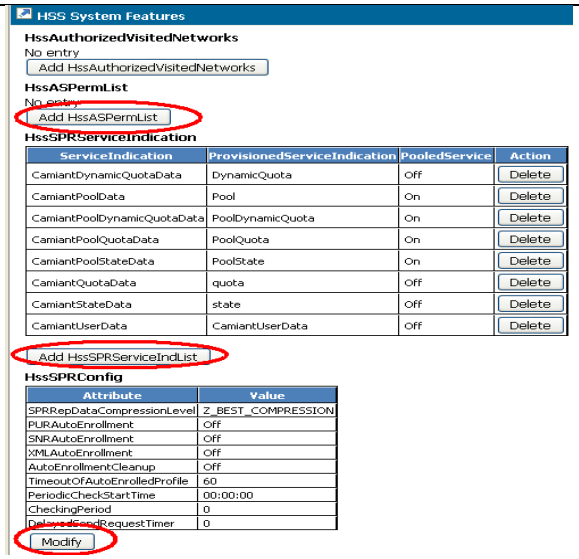


HssConfigDestinationRealm: To provision the domains only from which the connections are accepted.

Example: LocalRealm = ims.blueslice.com

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

Example: LocalFQDN = hss.ims.blueslice.com
</td>
</tr>
<tr>
<td>14</td>
<td>Configure HSS system features</td>
<td></td>
</tr>
</table>

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


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.

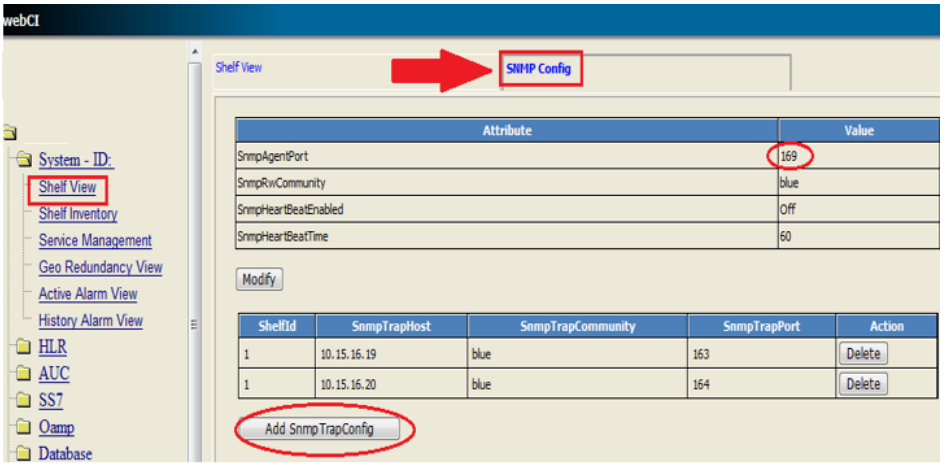
PURAutoEnrollment = **ON/OFF**

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**
</td>
</tr>
<tr>
<td>15</td>
<td>Configure the SNMP on 1st and 2nd SPR cluster</td>
<td>
Oracle Tekelec SDM™ → System - ID: → Shelf View → SNMP Config

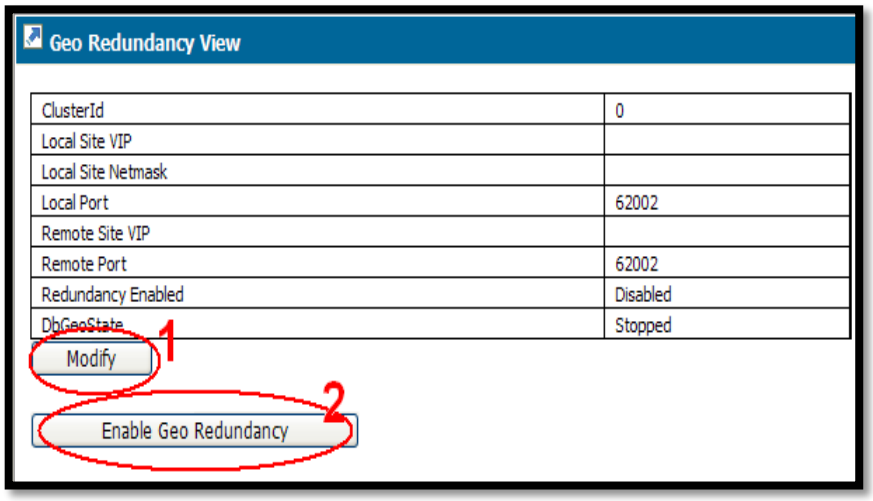


- Change SnmpAgentPort to 163
- Add Snmp Traps with customer information
</td>
</tr>
</table>

		• 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

10.0 GEO REDUNDANCY CONFIGURATION

Procedure 8. 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 TEKELEC 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 BASIC INSTALLATION AND CONFIGURATION OF SDM SOFTWARE. • 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 Tekelec 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 :

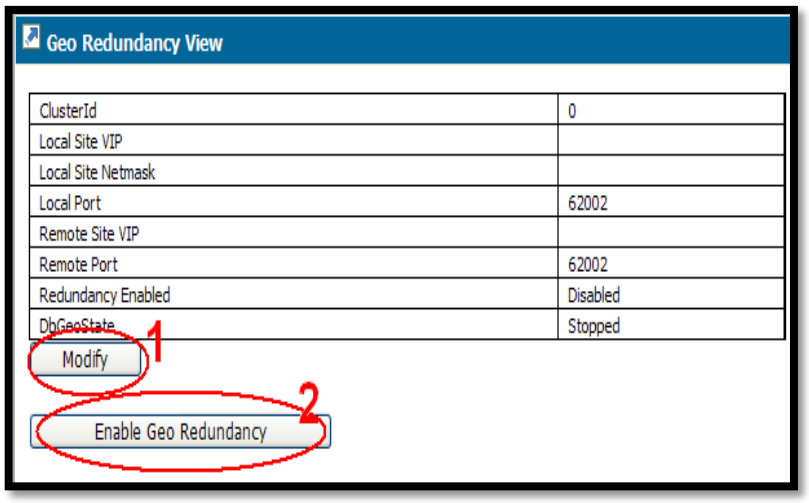
<table>
<tr><td>ClusterId</td><td>0</td></tr>
<tr><td>Local Site VIP</td><td>10.240.230.46</td></tr>
<tr><td>Local Site Netmask</td><td>255.255.255.0</td></tr>
<tr><td>Local Port</td><td>62002</td></tr>
<tr><td>Remote Site VIP</td><td>10.240.241.10</td></tr>
<tr><td>Remote Port</td><td>62002</td></tr>
<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 Tekelec 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 the 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 the WebCI in **SDM1**,Verify the current Geo Redundancy configuration :

Under System – ID => Geo Redundancy View :

ClusterId	0
Local Site VIP	10.240.230.46
Local Site Netmask	255.255.255.0
Local Port	62002
Remote Site VIP	10.240.241.10
Remote Port	62002
Redundancy Enabled	**Enabled**
DbGeoState	**ReferenceProtected**

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 :

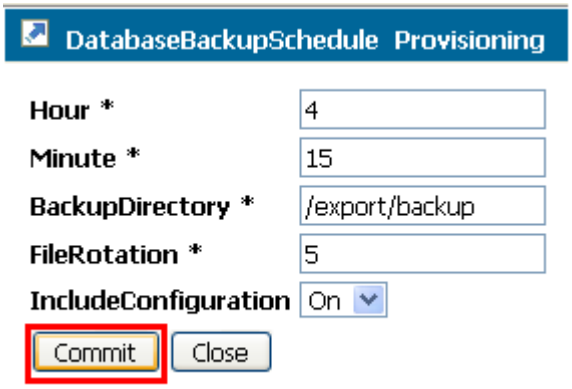
```
# /blue/usr/local/tungsten-replicator/tungsten-replicator/bin/trepctl services

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>

11.0 SDM SPR DATABASE BACKUP SCHEDULE AND NETBACKUP CLIENT CONFIGURATION

Procedure 9. 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:** • 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 [TK6] 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 TEKELEC 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 the 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

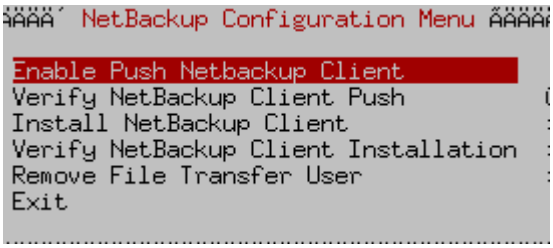
For more details on how to configure NetBackup client refer to [TK7] section 3.14.5 **Application NetBackup Client Procedures.**

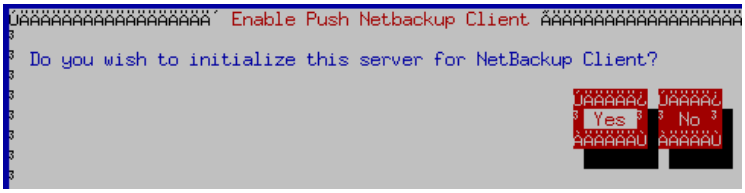
Depending on the Interconnect strategy ,additionnal lines might be added to sdm-vlans.conf file.Refer to Appendix C for interconnect strategy methods with Netbackup server on C-CLASS.Dedicated bandwidth is recommended.

Connect to platcfg menu :

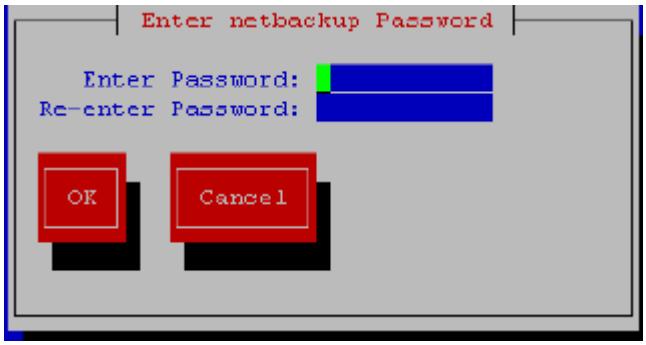
 # su – platcfg

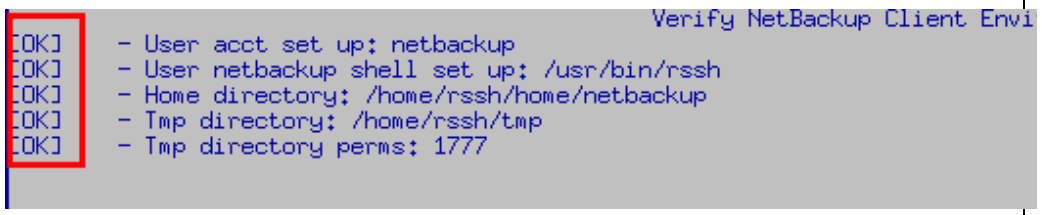
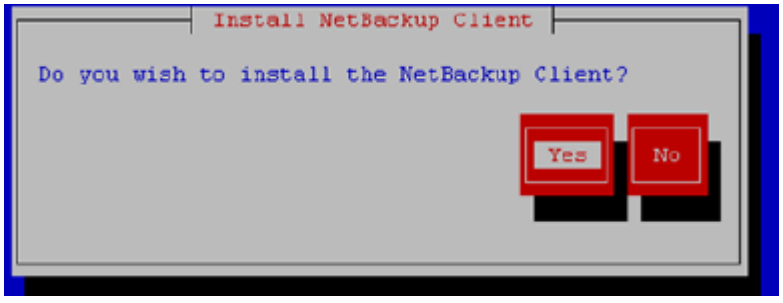
NetBackup Configuration → Enable Push Netbackup Client → Yes

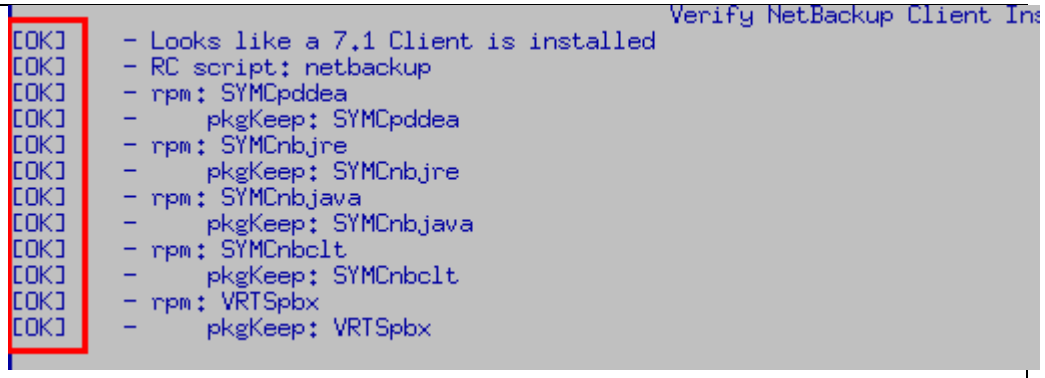




- Enter NetBackup password and select OK :



3 ☐	Verify NetBackup Client software push is enabled and update SPR hosts file	**NetBackup Configuration → Verify NetBackup Client Push**  • Update the application hosts file with NetBackup server info **# 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 **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
```

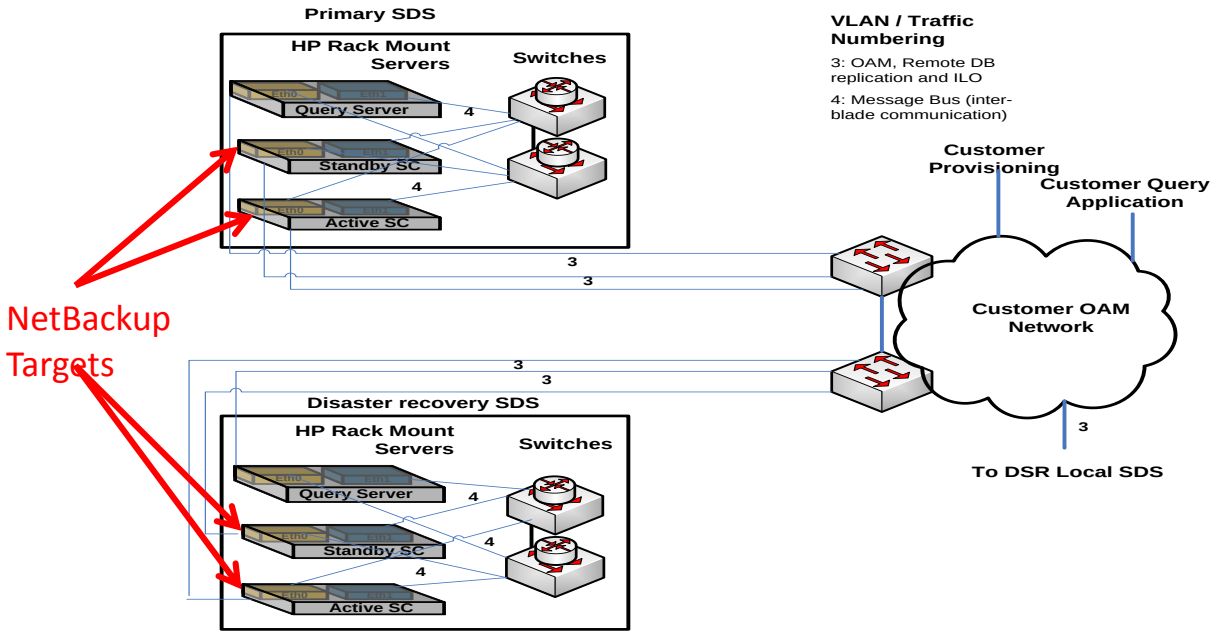
```
# should match the LOCAL-GROUP name used on the remote group.
#
# One or more remote VIPs may be associated with the remote group.
# These are VIPs that must be reachable as SSH destinations from any
# member in our local group.
#
# Typically, because of firewall or routing restrictions, there may
# 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

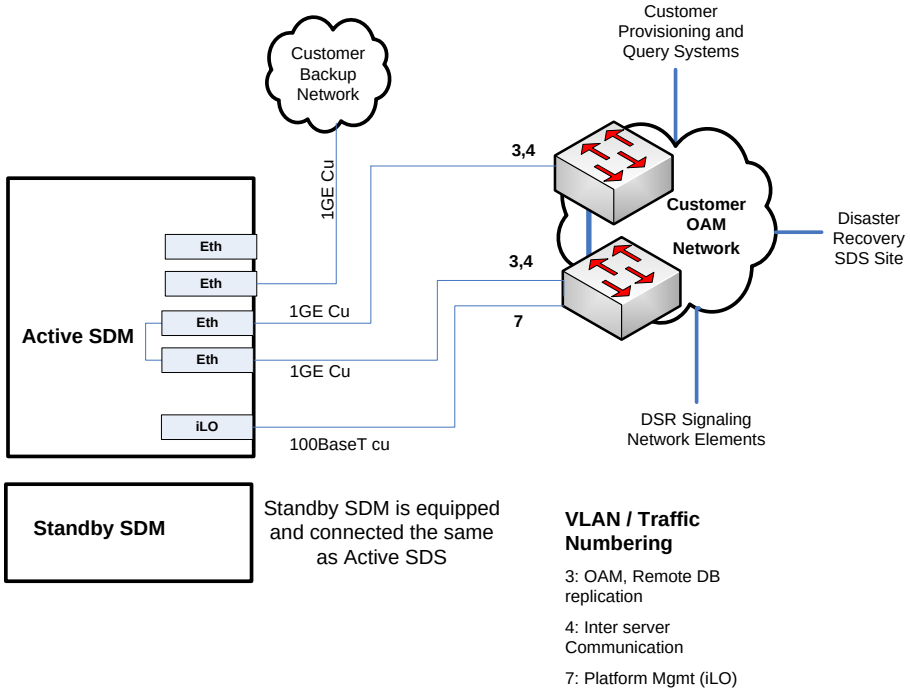
By default, backup activities would share the same bandwidth as XMI and XSI activities (method 1). This can lead to serious performance degradation during the backup time windows, while transfer of backups take place over the network.

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)